

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services and Communications Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p><b>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.</b></p>					
1. REPORT DATE (DD-MM-YYYY) 12-01-2008		2. REPORT TYPE Final		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE Defense Science Board 2007 Summer Study on Challenges to Military Operations In Support of National Interests; Volume 1 Executive Summary				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Dr. Craig Fields & Mr. Richard Haver, Task Force Co-Chairmen				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Science Board 3140 Defense Pentagon, Room 3B888A Washington, DC 20301-3140				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Science Board 3140 Defense Pentagon, Room 3B888A Washington, DC 20301-3140				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT A: Open Distribution					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 97	19a. NAME OF RESPONSIBLE PERSON Debra Rose
a. REPORT Unclass	b. ABSTRACT Unclass	c. THIS PAGE Unclass			19b. TELEPHONE NUMBER (Include area code) 703-695-4157

20090327438

**DEFENSE SCIENCE BOARD 2007 SUMMER STUDY**  
**Challenges to Military Operations**  
**In Support of National Interests**

Volume 1 Executive Summary • December 2008



*Report of the*  
**Defense Science Board**  
**2007 Summer Study**

# **Challenges to Military Operations in Support of U.S. Interests**

*Volume I*  
*Executive Summary*

**December 2008**

Office of the Under Secretary of Defense  
For Acquisition, Technology, and Logistics  
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB).

The DSB is a federal advisory committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

The DSB Task Force on Challenges to Military Operations in Support of U.S. Interests completed its information gathering in August 2007.

This report is unclassified and cleared for public release.





DEFENSE SCIENCE  
BOARD

OFFICE OF THE SECRETARY OF DEFENSE  
3140 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3140

9 Dec 2008

MEMORANDUM FOR: UNDER SECRETARY OF DEFENSE FOR  
ACQUISITION, TECHNOLOGY, AND LOGISTICS

SUBJECT: Report of the Defense Science Board 2007 Summer Study on  
Challenges to Military Operations in Support of U.S. Interests

I am pleased to forward the final report of the Defense Science Board 2007 Summer Study on Challenges to Military Operations in Support of U.S. Interests. The report offers important considerations for the Department of Defense in response to future threats to our nation's security.

This study, robust in scope, concerns itself with challenges the U.S. military might face in the future, emphasizing areas where the nation is less well prepared. Future adversaries are more likely to attack the nation with asymmetric tools of war, employed using non-traditional concepts of operation. Thus, challenges from nuclear weapons, from cyber warfare, in and from space, to force deployment and resupply, and on U.S. soil, may well dominate in the decades ahead. Addressing U.S. vulnerabilities in these and other areas is the focus of the study's effort, leading to actions for the Department that can improve the nation's posture against future threats.

I endorse all of the study's recommendations and encourage you to forward the report to the Secretary of Defense.

A handwritten signature in dark ink, reading "William Schneider, Jr.", is positioned above the printed name. The signature is fluid and cursive, with a large, stylized "I" at the end.

William Schneider, Jr.  
DSB Chairman



DEFENSE SCIENCE  
BOARD

OFFICE OF THE SECRETARY OF DEFENSE  
3140 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3140

MEMORANDUM FOR: Chairman, Defense Science Board

SUBJECT: Final Report of the Defense Science Board 2007 Summer Study on  
Challenges to Military Operations in Support of U.S. Interests

U.S. conventional military capability remains unmatched by any state. As a result, nations and powerful non-state actors, weaker in conventional weaponry, will face the United States with unconventional weapons. Further, these asymmetric tools of war may well be employed using non-traditional concepts of operation. And the battlefield may no longer be limited to regions afar, but may include the U.S. homeland. The United States could well confront the possibility of going to war abroad in the face of significant devastation in the homeland—dividing forces between homeland catastrophe relief operations and combat abroad—even facing the possibility that deploy and supply of U.S. military forces could be delayed and disrupted.

How to contemplate this future, over the next two decades, was the focus of the Defense Science Board 2007 Summer Study. The question asked by the study is this: **Is the United States maintaining its capability to deter and defeat a nation or non-state actor who might employ unconventional as well as conventional means, in non-traditional as well as traditional ways, to thwart U.S. interests?**

To focus on challenges for which the United States might be less well prepared, the study investigated seven topic areas, making recommendations for actions in each of them:

- **Future of war.** The character of war is changing—it is irregular, catastrophic, disruptive and no longer confined to the traditional battlefield. This changing character of warfare calls for considerations about how the nation's military capabilities should evolve—the type of forces, reliance on information infrastructures, protection to forces and critical infrastructure, new capabilities. At the same time, other instruments of national power must be brought to bear, which will involve strengthening relationships between the Department of Defense and other federal partners.
- **Unconventional weapons and technology proliferation.** The technology equation, between the United States and potential adversaries, is key to the nature of future warfare and the ability of our nation to prevail. The range of possible destructive weapons is vast, but three stand out as the most critical: nuclear weapons, biological agents, and cyber warfare. There are

steps that can be taken—in prevention, attribution, mitigation, and recovery—that can improve the U.S. posture against such attacks.

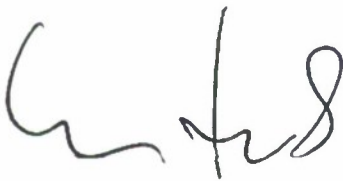
- **Nuclear proliferation—a special case.** The nuclear threat stands in a class by itself in terms of its potential for damage, disruption, and devastation. Thus, managing the challenge of nuclear proliferation deserves special attention. History has shown that it is possible to influence the decision to acquire nuclear weapons. Thus emphasis should be placed on developing tailored approaches to proliferation prevention to shape the nuclear environment. At the same time, the United States needs to prepare to cope with the military operational challenges of a more proliferated world—closing the sizeable gap between current capabilities and future needs.
- **Unconventional operational concepts and the homeland.** The capable adversary of the future will execute “one game”—attacking U.S. interests wherever the nation is most vulnerable, and that could mean the homeland. Overseas deployment, simultaneous with responding to a significant scale of attacks in the homeland, will stress DOD capabilities. Roles and responsibilities are not clearly defined, and adequate resources have not been invested in the homeland defense missions. Furthermore, the problem extends beyond DOD to the interagency and response communities, where the handoffs and roles are not well understood—in part because they are not effectively exercised.
- **What we know and don’t know about adversary capabilities: intelligence.** It is not possible to plan and prepare for all possible futures; nor is it possible for an adversary to exercise all of the opportunities to which they might take advantage. Thus, with good intelligence, the United States can focus its investments on the most likely cases. Strategic issues should command top level focus in the Intelligence Community, and the attention of some of its best resources. Improvements are also needed in foreign and domestic intelligence collection, analysis, and support; countering foreign intelligence; net assessments and gaming; and methods for improving intelligence related to the threat of weapons of mass destruction (WMD).
- **Fighting through asymmetric counterforce.** While the range of potential asymmetric attacks is wide, this study identified three as particularly challenging: conducting military operations in WMD environments, countering attacks on U.S. and allied space capabilities, and cyber warfare against information networks. DOD needs to take steps to enhance the capabilities of general-purpose forces to operate in an environment where WMD have been used. Further, the ability to operate in and from the global commons—space, international waters and airspace, and cyberspace—is critical to DOD’s ability to conduct operations and project power anywhere

in the world. Thus, the Department must act to mitigate vulnerabilities in these areas.

- **Strategic communication—another instrument of U.S. power.**  
Defending U.S. interests against future adversaries will require more than just military might—involving other instruments of U.S. power such as diplomacy, economic and financial sanctions, and strategic communication. Strategic communication is vital to America's future and must be transformed at strategic and operational levels. The range of future threats varies greatly and requires a strategic communication instrument with sustained impact and far greater capacity to understand, engage, and influence global populations on issues of consequence—an instrument that emphasizes actions that are consistent with what national leaders say.

Taken together, the issues addressed in this study point to the fact that the cost to deter or defeat future adversaries is rising—costs defined not only in financial terms but also along other dimensions to include military lives, civilian lives, money, civil liberties, daily comfort, economic health, and global reputation. Thus, instruments of national power, other than military, will assume greater importance.

The nation is unprepared and is making little progress in reducing these costs. But circumstances can be materially improved. The United States can achieve its national objectives by taking a combination of actions that will have an impact on costs—actions that are detailed in the recommendations of this report. DOD must begin to act, even as it fights the current war, to make sure it is ready for the next war, one that could well be even more stressing than the war the nation fights today.



Dr. Craig Fields  
Co-Chair



Mr. Richard Haver  
Co-Chair



# Table of Contents

## Volume I. Executive Summary

Major Themes.....	xi
The Future of War.....	2
Unconventional Weapons and Technology Proliferation.....	9
Nuclear Proliferation: A Special Case.....	20
Unconventional Operational Concepts and the Homeland.....	27
What We Know and Don't Know about Adversary Capabilities:	
Intelligence .....	42
Fighting Through Asymmetric Counterforce.....	46
Strategic Communication: Another Instrument of U.S. Power.....	57
Final Thoughts .....	70
Terms of Reference .....	73
Study Participants.....	77
Presentations to the Study .....	85
Glossary.....	97

## Volume II. Main Report

Part I. The Future of War
Part II. Unconventional Weapons and Technology Proliferation
Part III. Nuclear Proliferation: A Special Case
Part IV. Unconventional Operational Concepts and the Homeland
Part V. What We Know and Don't Know about Adversary
Capabilities: Intelligence
Part VI. Fighting Through Asymmetric Counterforce
Part VII. Strategic Communication: Another Instrument of
U.S. Power

## Major Themes

**Nations and powerful non-state actors, weaker in conventional weaponry, will face the United States with unconventional weaponry. The most challenging are:**

- nuclear weapons, worsened by proliferation
- self-replicating biological weapons
- cyber weapons to disrupt net-centricity, including in space

**They will also exploit vulnerabilities in our homeland security by:**

- attacking our homeland to disrupt military deployment and supply
- dividing our joint forces between domestic civilian relief and foreign military operations

**We are unprepared:**

- At best, our policies and actions will be severely constrained.
- Worse, we will enter the fray and then quit when we come to appreciate the full cost of success.
- These costs are defined not only as financial costs, but also along broader dimensions, such as military lives, civilian lives, money, civil liberties, daily comfort, economic health, and global reputation.

**Instruments of national power other than the military, such as strategic communication, will assume greater importance.**

## Executive Summary

U.S. conventional military capability remains unmatched by any state. As a result, no adversary—peer, near peer, or powerful non-state actor—with objectives in conflict with U.S. interests will oppose our nation with conventional military means. The United States is too strong and capable. Yet, this strength in the conventional arena does not mean that the nation is unmatched across the spectrum of conflict.

The proliferation of technology, technical information, and technical skills facilitates access to a range of weaponry, other than conventional, that can be used to attack the United States both at home and abroad. These include weapons of mass destruction (WMD), such as biological, chemical, nuclear, radiological, electromagnetic pulse, directed energy, and high explosives, as well as cyber warfare. No longer are adversaries limited to nation states. Technology proliferation has afforded access to the tools of warfare to non-state actors, such as terrorists, insurgents, and groups not bound by geography and the traditional trappings and vulnerabilities of statehood.

These asymmetric tools of war may well be employed using non-traditional concepts of operation. Moreover, the battlefield may no longer be limited to regions afar, but may include the U.S. homeland. The United States could well confront the possibility of going to war abroad in the face of significant devastation in the homeland—dividing forces between homeland catastrophe relief operations and combat abroad, or even facing the possibility that deploy and supply of U.S. military forces could be delayed and disrupted.

How to contemplate this future over the next two decades was the focus of the Defense Science Board 2007 Summer Study. The question asked by the study was this:

**Is the United States maintaining its capability to deter and defeat a nation or non-state actor who might employ unconventional or conventional means, in non-traditional as well as traditional ways to thwart U.S. interests?**

The study, necessarily robust in scope, concerns itself with challenges the U.S. military might face in the future for which the nation is less well-prepared. To approach the investigation into U.S. capabilities, capability gaps, and necessary actions to improve the nation's ability to prevail against the future described herein, the subject matter was divided into seven topic areas, with no attempt to ensure that they were mutually exclusive. Each is treated in turn in the summary that follows.

- the future of war
- unconventional weapons and technology proliferation
- nuclear proliferation, a special case
- unconventional operational concepts and the homeland
- what we know and don't know about adversary capabilities: intelligence
- fighting through asymmetric counterforce
- strategic communication: another instrument of U.S. power

## The Future of War

---

For five centuries, it has taken the resources of a state to destroy another state. For nearly two centuries, the U.S. homeland has been immune from attack (with the exception of Pearl Harbor). It has been a quarter of a century since the United States had a serious peer competitor. However, things are changing. The globalization of transportation and communication; over-dependence on a vulnerable, interconnected infrastructure; increasingly affordable weapons of mass destruction; and the likely emergence of a near-peer promise new challenges to the nation's security.

In fact, challenges of the sort anticipated in the future are already occurring to a certain degree (Figure 1). Plots to kill U.S. soldiers at Ft. Dix and cyber attacks in Estonia are suggestive of the type of asymmetric tools and tactics that could be employed. China's exploration into unrestricted warfare has been widely publicized. And the challenges the nation has faced recently in responding to domestic catastrophes while fighting abroad illustrate the reality of how difficult it can be to allocate scarce resources to meet U.S. interests both at home and abroad.





**Figure 1.** The First Glimpse that It's Already Happening

What is a peer or near-peer competitor? A peer or near-peer is any adversary, or network of adversaries, whose capabilities are such that in a supreme test of wills with the United States, the outcome is uncertain. The peer relationship—military and/or economic—might be symmetric, where their capabilities mirror those of the United States, or asymmetric, where their strengths play to U.S. weaknesses. A peer's instruments of national power need not be at parity with our own, even in the symmetric case. It is really a question of whether, in such a context, the United States could prevail at an acceptable cost. History shows that in a contest between nations the winner is not necessarily the most endowed nation, but the one whose government can muster and sustain the necessary treasure and commitment from its people.

The U.S. military is presently engaged in stabilization and reconstruction efforts in Iraq and Afghanistan, combating terror and facing up to the global challenge of radical Jihadists. Despite these preoccupations, or perhaps because of them, it is important to ask whether these are independent actions, or of a larger piece, and whether this is the future or merely an interlude "between wars." The degree of effort, mental and physical, focused on these immediate concerns, is perhaps distracting the United States from more serious potential conflict.

At the conclusion of the current deployments, the United States will take the opportunity to “reset the force.” The question looms: reset for what eventualities—a reprise of recent events, a return to major power standoff, major regional or even global conflict, or something new and as yet inexperienced? To answer these questions this study began with a review of U.S. military history to identify trends that could extrapolate into the future. It also considered plausible scenarios that, unanticipated, could confound the U.S. military. And in the context of future scenarios, another question emerges: what does it mean to win in the future? The answer, from this study’s perspective, is that winning or losing is defined by whose national interests prevail and whose military objectives are met.

If that is what defines winning, an important element is “at what cost.” National objectives enabled by military prowess have certain value but incur certain costs. The cost equation is changing. Nations and powerful non-state actors are raising the “cost” of employing military force to support national interests. Some, like materiel costs, are calculable in dollars. But there are other costs as well—human life, depletion of moral capital, infringement on the rights of the citizenry, economic health, global reputation—and these are harder to measure. We, as a nation, must either pay the cost or find ways to reduce it.

In general, things that the nation fails to anticipate and, in turn, does not prepare for, distort the cost equation disproportionately. If the nation is able to anticipate adversary strategies to increase costs, it may be possible to develop new weapons and tactics to counter those strategies and reduce costs.

### ***Potential Game Changers***

The character of war is changing. The 2004 Defense Strategy and subsequent Quadrennial Defense Review identified four categories of war—traditional, irregular, catastrophic, and disruptive—arguing that, given the U.S. dominance in the first category, future adversaries would focus their strategies on the others. While there is no scientific approach to determine the future, several developments are anticipated.

#### **Irregular Warfare**

Likely to be especially troublesome to the United States is the “hybrid” complex irregular warfare that combines state-like capabilities—more sophisticated missilery and anti-armor systems, armed unmanned aerial vehicles, and signals intelligence—with skillful guerilla warfare. Nor is there reason to

think that a future peer would restrict military competition with the United States to “traditional” warfare. Complex irregular warfare has political dimensions, too, and exploits “lawfare”—the use of rules of engagement against the United States (while ignoring those rules, themselves). Another non-traditional form of warfare may involve manipulation of the media, which tends to be to the advantage of U.S. adversaries who are willing to engage in spectacular acts (generally involving loss of life) that attract media attention.

### **Nonlinear Battlefield, Including the Homeland**

For years, U.S. military planners have predicted the “nonlinear battlefield” in which the concept of the forward line of troops goes away. In fact, that has already happened. In Iraq today, for example, combat forces are dispersed to many locations with potentially hostile areas in between them. There is no single “line,” and no large secure rear area. In the future, the situation is likely to be even more complex, as what the United States has traditionally regarded as completely secure (the homeland), becomes a target, as well as the homelands of many allies. The commander in such a context must have a 360-degree view and must operate without the luxury of simple demarcations.

It is unlikely that future U.S. military engagements can be limited to a geographically isolated theater of operations and a well-defined forward edge of battle. The front line has been replaced by a 360-degree battlespace. Military technology increasingly affords medium- and high-end conventional adversaries the reach to leap over traditional battle lines and into the U.S. heartland, no matter where the primary clash of arms is located. Moreover, both traditional (i.e., symmetric) and irregular (asymmetric) adversaries can achieve such reach using the commercial infrastructure and technology of globalization to reach “behind the lines.” This is especially true when cyber warfare is a component of the battle, since “cyber-space” does not map at all well into geography.

Potential adversaries have studied U.S. military operations, dissecting doctrine, strategy, and tactics. They are remarkably adaptive at imposing cost-incurring strategies upon the United States. The expeditionary nature of the U.S. military faces an increasing challenge from over-the-horizon targeting, quiet diesel submarines, anti-ship missilery, and related technology. As the launch point for a projecting force moves further from its target, the challenges multiply.



### **Technology Innovation**

The relentless advance in technology will be another factor in future warfare. The United States, for a long time, led in the development and application of new technologies to the battlefield. This occurred largely because investments in military technology have been expensive and the United States has been able and willing to make the required investments. The fruits of technology have been greater efficiency and, thus, lower cost. This is especially true as technological advancements migrated from heavy industry to information technologies. In either case, the buy-in cost for opposing forces has lowered dramatically.

Today, off-the-shelf weaponry and/or easily adaptable commercial technologies enable a less-resourced, but more agile adversary to catch up and sometimes to pull ahead. Moreover, most improvements in technology can be seen to favor the asymmetric offense of certain adversaries and U.S. defenses suffer by comparison. Certainly this is true for offensive WMD technologies—chemical, biological, and nuclear. Technology is continually making them cheaper and more potent, but technology has comparatively low yield for defense against these agents. Note, too, that the United States does not benefit from offensive improvements because our nation is self-restraining—a double-edged sword.

### **Information Space as a Battlefield**

Asymmetries in information space derive from U.S. reliance on information technologies for command, control, computing, communications, intelligence, surveillance, and reconnaissance (C4ISR). “Cyber-war” can be a low-budget affair for many adversaries, wreak substantial havoc on U.S. operational capabilities, and be relatively immune to a response in kind, insofar as no adversary depends as much on their information technology infrastructure.

Absent strong measures the United States could be the victim of its own success in information technologies, especially C4ISR, that enable speed of maneuver and synchrony of action. The use of technological advances against the nation will almost certainly mean that some of the gains implicit in net-centricity and the commercial-off-the-shelf revolution will be lost. Getting serious about information assurance is necessary, but not sufficient; it is necessary to reduce, or offset, over-reliance on information systems.

An interesting characteristic of some cyber “weapons” is that they are “self-replicating” and generally “self-deploying,” traits they share with biological weapons. While nuclear weapons may be the “ultimate” weapon of mass



destruction, radiological the most obtainable, and explosives the old standby, the self-replication of both cyber and biological weapons make them especially fearsome. Coupled with their increasingly lower buy-in costs, they are especially attractive to the would-be adversary. Restraint has been the hallmark of biological, chemical, nuclear and, so far, radiological weapons, while explosive and cyber attacks are a daily nuisance. Can this state of affairs continue?

### **We Still Have Nuclear Weapons**

Through the latter half of the 20th century, nuclear weapons held a special place in nation-state warfare. Used only twice in anger, they forced an adversary's capitulation in the world's worst conflict and played a powerful role in deterring further conflicts of that scale. They allowed us to extend deterrence to allies, empowered our foreign policy, and restrained it, as well. Deterrence and restraint stemmed from the parity we consciously sought with the Soviet Union and our own sizeable, capable nuclear arsenal. Despite their fears, most Americans came to believe, correctly, that, should it ever come to that, our nuclear weapons could be relied upon to do the job.

In the case of nuclear weapons, the future may depart from the past. Worrisome evidence suggests the "nuclear club" could expand substantially, inasmuch as many are viewing it as a cost-effective counter to U.S. conventional superiority. Proliferators conceivably could include some non-state actors. Current U.S. policy dictates that our nuclear arsenal is stuck in time—aging and of uncertain but likely declining reliability. Our delivery systems are approaching end-of-life and our weapons inventory is shrinking in number and variety, constraining alternatives in the event of operational reliability problems. Contrast this with other key nuclear-capable nations who are modernizing substantially their nuclear weaponry and couple it to a future in which the number of nuclear-capable actors may double or triple.

Our lack of nuclear weapons production capability—and our stricture against not only development, but design—holds our future hostage. Reestablishing such capacity from a standstill would be a very lengthy process, perhaps ill-matched to the pace of world events. We will have lost personnel and unique skills as well as physical plant and production know-how for a generation, or two.

This atrophy and the relative diminution of our nuclear capability may call into question America's ability to deter, extend that deterrence, and to prevail, in the event. It could embolden others and change the future of warfare to our

dismay. To secure our place may require reliable replacement warheads as well as new designs for new missions that uniquely require powerful weapons such as to destroy, with certainty, a deeply dug WMD facility.

Recommendations here are hard to come by. Starting sooner to reverse any decline rather than postponing endlessly could prove important but calibrating the urgency is ever so difficult. Rightly, our policy on nuclear testing consigns us to uncertainty about reliability and intelligence can be unreliable in gauging perceptions of adversaries. Indeed, what matters most is the certainty our decision-makers have that our arsenal could do the job and the uncertainty of the adversary that it cannot—perception, vice fact. Curiously, unless we have the capacity to promptly rectify the situation, a resumption of testing could work to our disadvantage should our expectations not be met. We know how long it would take to regain lost momentum should we choose, and we should take measures to reduce that lead time.

### **Impact on Civilians**

A tentative forecast is that the impact of war on civilians will increase. War in the 21<sup>st</sup> century may be less murderous than in the 20<sup>th</sup> century, but armed violence, creating disproportionate suffering and loss, will remain endemic—occasionally epidemic—in a large part of the world. But the importance of this expectation is the fact that many adversaries have a different perspective toward civilian deaths than does the United States. For the United States, civilian deaths are a negative aspect of war. For some adversaries, their view may be neutral or even positive. Their objective may well be to increase civilian deaths, amplified by the impact of such casualties on the media. One death or casualty “on camera” has the impact of hundreds of actual casualties.

### ***Preparing for the Future***

Although U.S. conventional prowess is unmatched, the increasing cost in blood and treasure of military interventions argues against use of the military to protect each and every U.S. interest. Prioritization and realism are essential. The changing character of warfare calls for considerations about how to balance the force—special forces versus general forces; about planning and preparing for degraded C4ISR capabilities; about force protection and critical infrastructure in the homeland; about the capabilities needed to fight through an attack using weapons of mass destruction; about new intelligence requirements.

At the same time, other instruments of national power must be brought to bear and the Department must make good on its promise to strengthen its other federal partners (Figure 2). Attributes of the military's "organize, train, and equip" capabilities could well be brought to bear in the interagency environment—capabilities such as discipline and organization; obligation to duty; command and control; planning, training, and exercises; and resourced for contingencies. The full-spectrum of homeland defense requires civilian defense partners that are disciplined, organized, and resourced.



Figure 2. The Inter-Agency at War

## Unconventional Weapons and Technology Proliferation

The technology equation, between the United States and potential adversaries, is a key element in evaluating U.S. capabilities to effectively and successfully wage war in the future. Access to technology will have a critical impact on the future battlefield. As a result, the study placed significant effort on understanding adversary use of various technologies in developing weapons, the technical issues underlying such development, and how the United States might combat that use.



There are many ways an adversary might attack. Nuclear weapons are not the only means by which an adversary can cause mass destruction or disruption. Used effectively, high explosives can have tremendous destructive power. Destruction of the Hoover Dam, for example, would destroy irrigation of one million acres of U.S. farmland, deprive 22 million U.S. citizens of water, and eliminate over 50 percent of the electrical power in southern California. Thus, eight destructive modalities, capable of achieving such effects, were evaluated: nuclear, radiation dispersal devices (Rad), biological (Bio), cyber warfare, chemical (Chem), high explosives (HE), electromagnetic pulse (EMP), and directed energy (DE).

What the adversary will do depends not only on the technologies available but also on the strategic objectives to be achieved. Strategic objectives might range from increasing hegemony in a new region to eroding political support for continuation of a war effort conducted by the United States and its allies. Strategic objectives could also be directed toward attacks on the homeland to diminish U.S. ability to deploy and resupply troops abroad or even to attack the U.S. civil infrastructure and population.

Because the range of possible technologies, the ways in which they might be used, and the spectrum of strategic objectives is so vast, the study evaluated subsets of these factors in an attempt to identify the most likely options an adversary might employ while, at the same time, considering the consequences of such attacks on the United States. The result of this assessment, for 20 generic attacks, is illustrated in Figure 3.

Such an assessment is important because the United States must make choices in how to invest resources to best prepare for such a future. It is simply not possible to prepare for each and every possibility that might arise. In the judgment of this study, when comparing the attractiveness of weapon alternatives to the adversary against the consequences of their use against the United States, its allies or friends ("blue"), the most critical modalities are: nuclear weapon, biological agents, and cyber warfare. Examples of how attacks using these three modalities might play out, what the United States can do in response, and what can be done to improve the U.S. posture in the future are described below.



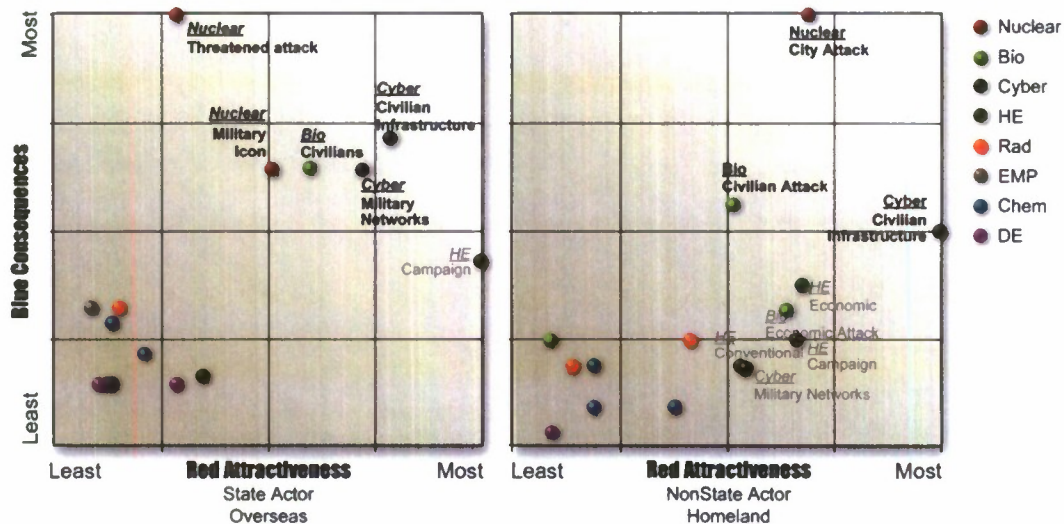
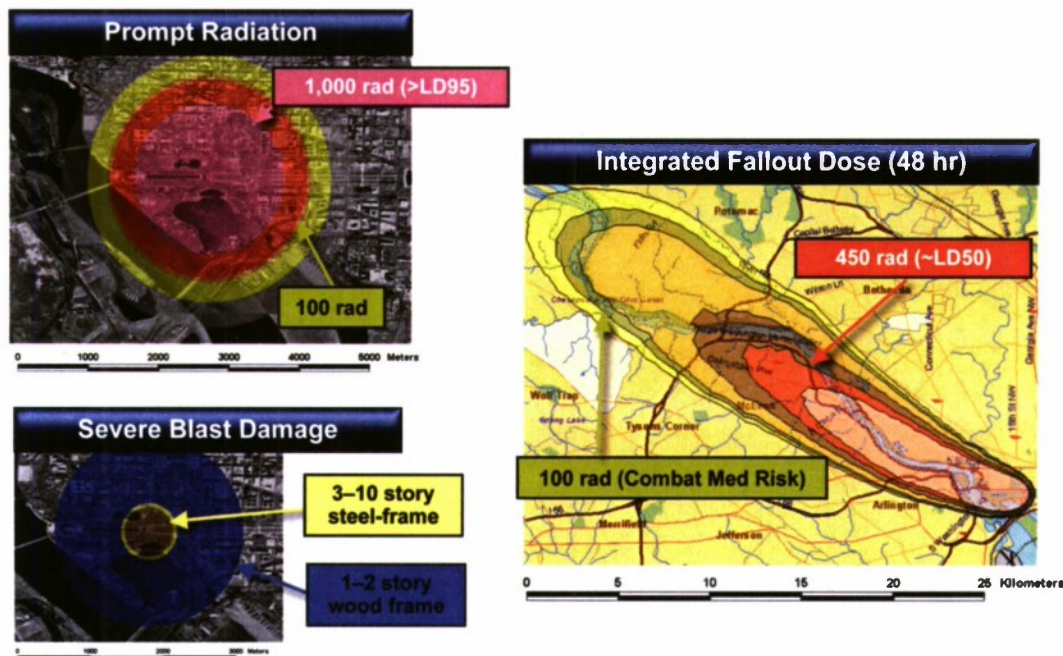


Figure 3. Assessing Adversary Attacks: Nuclear, Bio, and Cyber Stand Apart

### *Nuclear Weapons*

Nuclear weapons are in a class by themselves due to their destructive power. But access to such weapons is not as difficult as one might imagine. Modern nuclear weapons are small and transportable. Weapon design is well documented in the open literature. With access to special nuclear material, weapons can be easily manufactured.

To understand the destructive power of nuclear weapons, consider a nuclear attack on an urban area in the United States. Such an attack could be motivated by a terrorist group that wants to enhance their status by creating a spectacular event in the U.S. homeland. How might it come about? A non-state actor acquires or improves a nuclear weapon. The weapon could be delivered via non-conventional means such as a small private vessel, aircraft, or SUV-sized vehicle. A surface burst would maximize fallout casualties. The attack would be unannounced followed by threats of additional detonations, with technical countermeasures employed to confuse attribution. Such an attack, using a 10 kiloton yield weapon detonated on the ground in the evening, could result in total fatalities of 40,000 persons, with 80,000 casualties (Figure 4). Daytime levels would be much larger. This size weapon is a reasonable size for a terrorist or state surrogate to obtain.



Source: Compiled by Defense Threat Reduction Agency

**Figure 4.** 10 Kiloton Surface Detonation of a Nuclear Weapon, Washington D.C.

A “blue” response falls in three areas—prevention, mitigation, and attribution and response. Emphasis should be placed on prevention programs, but the nation should be prepared to respond. The primary effort to reduce the nuclear threat to the United States is on *preventing* nuclear weapons from getting into the hands of adversaries who are not likely to be deterred by cold-war approaches. The critical steps to address this goal include the improvement in security—such as the deployment of mobile detection networks during heightened alert—and the drawdown of existing fissile material stocks. Programs in these areas include securing special nuclear materials that are most at risk in Russia; strengthening international standards to secure weapons-usable nuclear materials, including those in transit; and developing nuclear reactors to burn weapons-usable nuclear materials.

In the *mitigation* area, protocols to guide situation awareness and action by local responders are needed. These protocols should be formulated and exercised with federal assets charged with supporting the response. Mitigation therapeutics can minimize radiation effects provided they are administered within about twelve hours of radiation exposure. More research in this area could save many lives should such an attack occur.

Attribution and response capabilities are no less critical. If a non-state actor acquires a weapon, it will often be with the support of a state sponsor to provide the necessary technological support or fissile material. Technical forensic activities following a detonation can assist in identifying the perpetrator of an attack as well as those who assisted in the design or acquisition of materials for the weapon. The robustness of these forensic processes should be improved, both by shortening the timelines associated with the rad/chem analyses central to the technical analysis, and by improving the databases used to identify the source of the materials following the analyses. The overall crisis action system to guide national response decisions based on technical forensics and other attribution information should be exercised, using realistic constraints so that decisions on retribution and international action can be swift.

In addition to current efforts to prevent proliferation and otherwise reduce the probability of a nuclear attack, recommendations emphasize two areas: attribution and consequence management. It is these areas where the nation is most underinvested and where DOD is a major player.

#### RECOMMENDATION: NUCLEAR

***Attribution.*** Develop post-detonation attribution capabilities to enable initial national assessment of responsible parties within 48 hours after attack:

- Defense Threat Reduction Agency (DTRA) to assume responsibility for robustness of post-detonation technical forensics; triple current budget of \$10 million in fiscal year 2007 for this mission.
- Intelligence Community populate nuclear materials databases per NSPD-17, Annex IV<sup>1</sup>
- U.S. Strategic Command/DTRA to plan and execute realistic response exercises with senior leadership, reflecting constraints and uncertainties of realistic attribution environment

***Consequence Management.*** Post-detonation consequence management goal is local capability for major U.S. cities for initial one-to-three days of response:

---

1. National Security Presidential Directive 17, on "National Strategy to Combat Weapons of Mass Destruction." Issued 11 December 2002.



- Deputy Secretary of Defense direct the National Guard to work with local authorities to ensure detailed response plans (radiation hazards, shelter/evacuation decisions, pragmatic decontamination for thousands of people)
  - Exercise with National Guard Civil Support Teams and U.S. Northern Command assets upon completion of plans
- 

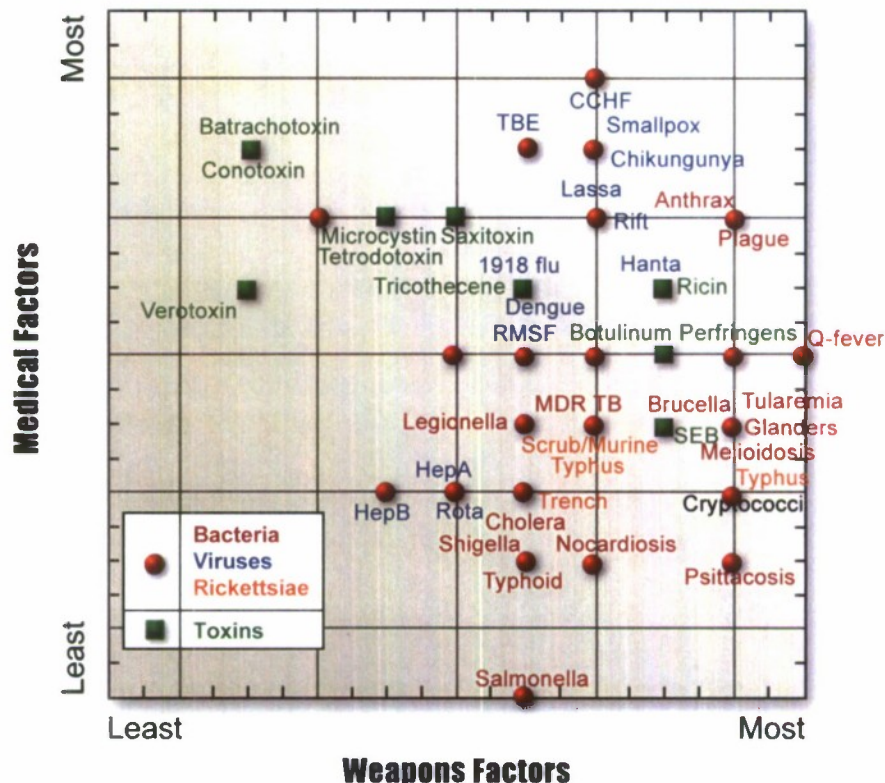
### ***Biological***

A great variety of materials (pathogens and toxins) could be employed for a biological attack. The effectiveness of actually using these many materials in a biological attack is a function of a biological material's characteristics and how they would suit a particular release scenario (Figure 5). Medical factors to consider include infectious dose data, virulence and lethality, diagnosis, and treatment. Weapons factors include stock availability, weaponization, dissemination, and persistence. Materials such as anthrax, small pox, and ricin rank high with respect to potential as an agent. However, under certain circumstances, lower ranked materials (such as salmonella, shigella, or *E. coli* released in food or water) could pose a formidable threat.

With the availability of so many materials, there is clear potential for an increased bio threat in the next five years using modified or engineered bio materials. For example, a biological attack could involve the use of bioagents against deployed military targets, strategically releasing bioagents to debilitate troops and diminish U.S. military effectiveness and strength. The most effective approach would be multiple releases of a variety of agents to contaminate vulnerable food and water supplies and/or contact infection of troops. By using a lot of different agents, each release is different.

Potential agents might include norovirus, salmonella, shigella, *E. coli*, protozoan parasites, and toxins such as botulinum or ricin. The characteristics of such a threat make it easy to prepare for frequent, successive multiple attacks that could yield profound effects. Stocks of these agents are available worldwide; they are easy to produce and disseminate; the effective dose is low; illness is debilitating and prolonged, even potentially fatal (toxins); and they require minimal equipment and training. Furthermore, the use of multiple organisms and their confusion with naturally occurring disease could make attribution difficult.





Compiled by MIT Lincoln Laboratory

**Figure 5.** Ranking Biological Threat Agents

From “blue’s” perspective, *prevention* is unlikely since it would require strict control of a variety of possible sites that could be accessed for agent release—food, water, air, and local populace contact. Simple control measures, such as chlorination and controlled supply chain, could minimize the effect of intentional or natural introduction of multiple pathogen types.

Rapid diagnostics and therapeutics could be employed to *mitigate and recover* from an attack. DOD needs to maintain an arsenal of rapid diagnostics for endemic and opportunistic pathogens. Other steps include expanding access to existing real time PCR, isolating infected troops quickly, maintaining treatment stockpiles, and investing in portable ventilators and other palliative care methods. Over the longer term, there is a need to develop smart tools for the field, such as rapid diagnostics for high-likelihood diseases, using techniques such as immunoassays, protein microarrays, fast DNA microarrays, and wearable soldier health-status sensors for early detection.

Attribution and response could be difficult to achieve in the event of multiple attacks with different biological agents or confusion with naturally occurring pathogens. Bioforensics and global reference databases are needed to distinguish released agents from natural pathogens and identify the attributes of the agents (virulence, drug resistance). In essence, focus is needed on rapid, treatment-directing diagnostics and other tools that can minimize the impact of attack.

#### RECOMMENDATION: BIOLOGICAL

***Interdiction.*** DTRA/Joint Program Executive Office (JPEO) to develop sensor networks in critical enclosed spaces of DOD (such as critical command, control, and communication nodes) for real-time triggers/identifiers integrated with heating, ventilation, and air conditioning systems to control and contain contamination.

***Mitigation.*** Assistant Secretary of Defense for Health Affairs advance DOD medical surveillance and response program for biological attack and coordinate with civilian program.

- Rapid diagnostics and networked reporting to contain/control
- Rapid distribution of treatments/prophylaxis (1-2 days)

***Attribution.*** Under Secretary of Defense for Acquisition, Technology & Logistics (USD (AT&L)) expand earlier Defense Advanced Research Projects Agency (DARPA) bioforensics/global reference database to identify specific bioagents and attributes.

***Recovery.*** USD (AT&L):

- Expand earlier DARPA programs for standoff mapping of contaminated surfaces using laser-induced fluorescence detection systems, SERS-coated nanoparticles, and colormetric foam
  - Continue development of diagnostics and broad-spectrum antimicrobials/vaccines and effective decontamination systems (DTRA/DARPA/JPEO)
-

## *Cyber Warfare*

Computer network operation is the third of the most critical modalities. Elements of cyber warfare include computer network defense, computer network exploitation, and computer network attack. Against a sophisticated adversary, the state-of-the-art in information assurance is significantly outmatched. The United States does not overpower the potential peer adversary in cyber warfare in the way it does currently in conventional military power. The best defenses and closely coupled offense—known as active defense—will mitigate the impact of a concerted attack by an adversary. But cyber warfare attacks are ongoing.

Net-centric warfare creates a dependence on remote sensors and services, making the Global Information Grid (GIG) an attractive cyber warfare target. Because the GIG employs commercial off-the-shelf hardware, malware introduced in manufacture or early in the supply chain could be widely disseminated. When triggered, the malware could disable much of the U.S. command and control network and destroy confidence in what remains. Combining such an attack with potential use of directed energy or electromagnetic pulse and selected high explosive attacks would be even more devastating.

Preventing such attacks is unlikely because there are seemingly infinite points in the GIG for an adversary to gain access either by successful penetration or by an insider. Upon gaining access, it is not difficult to propagate mischief more broadly. Efforts to mitigate attacks are difficult as well, but could be successful. For the nations' most critical systems, protection of some supply chains may be needed in view of offshore production of information technology components. Another approach is to design and operate cyber systems for assured capabilities. Designing these systems to degrade to protected citadels, perhaps akin to wartime reserve modes, is an important approach, but a difficult one to achieve. Critical to effective operations in the wake of a cyber attack is to test and exercise operations in a degraded mode so that troops learn how to operate under such circumstances.

U.S. reliance on effective information technology, especially in C4ISR systems, places huge premiums on the integrity of system data at all times. Thus, an ability to recover and reconstitute data integrity will be crucial and must be part of the initial design of system development. Some elements of such capabilities include hot back-up for critical systems, highly trained systems administrators, dynamic encryption/re-encryption, and out-of-band order wire.

Today there is no effective deterrence to limit or prevent adversary attacks. Attribution and response, while critical, are particularly difficult. Some work is

ongoing regarding attribution, but great success is not forecasted. Further, permission for active cyber response is held at the most senior levels of government. An important element in the recommendations put forward is the need to make tough choices in designating systems as “mission-critical.” These systems need to be treated, designed, and built differently, and they need to be the focus of exercises and operational tests. Without making such choices, resources that can be devoted to information technology security will be spread around equally and too thinly, and result in countermeasures with little or no effectiveness.

#### **RECOMMENDATION: CYBER WARFARE**

**Identify DOD’s mission-critical systems and make their protection a priority:**

- The Y2K process model for identifying and ranking critical systems could serve as a model for the selection process.
- Design, build, test, exercise, and operate differently, beginning early in the acquisition cycle, during operational test and evaluation, and continuing through the life cycle. Make extensive use of red teams throughout the process.

**Educate industry on its vulnerabilities and adversary capabilities, to the extent possible.**

---

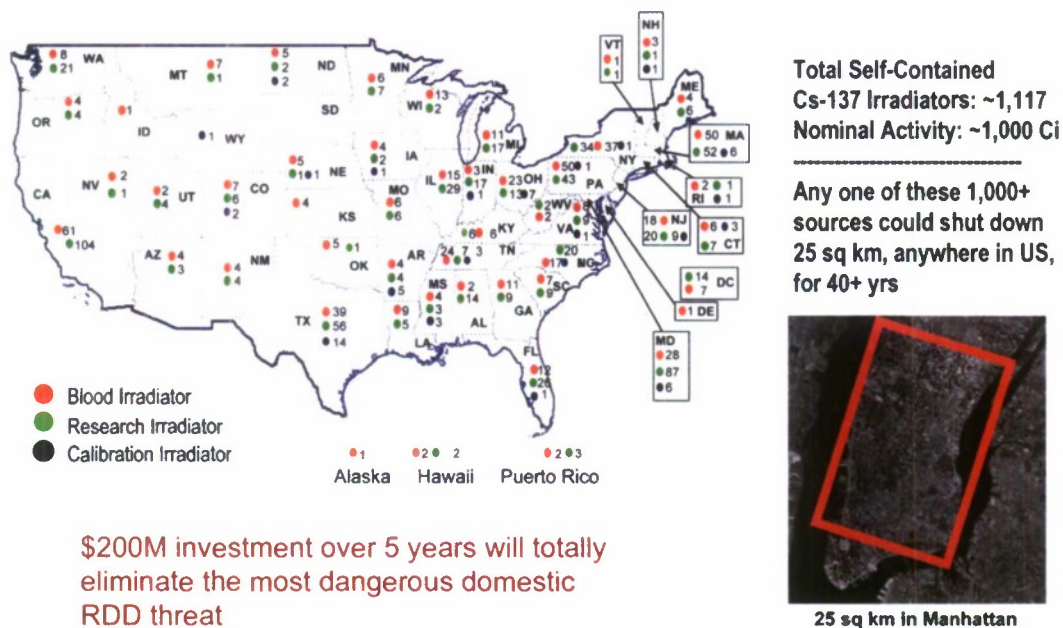
#### ***Other Modalities***

In addition to the single modality attacks described as examples of what a potential adversary could initiate, multiple, coordinated attacks are possible as well. Such attacks could take many forms. One is an attack using multiple modalities. An example might be multiple attacks on U.S. satellites using directed energy attacks to blind the satellites and jam communications, high-explosive attacks against the uplinks, and cyber attacks against any component of the architecture. Another form might be a sequence of attacks using a single modality, such as high explosives, where the impact of each successive attack becomes more devastating.



Thus, to raise the bar for other modalities, the best approach is to focus on large-scale events and campaigns. The study recommends that the Under Secretary of Defense for Policy (USD (P)) advocate an interagency program to strengthen regulatory control processes for stock substances, such as bio, chem, hazardous materials, and high explosives. Also, the Under Secretary of Defense for Intelligence should coordinate with the Director, National Intelligence, to identify and track critical weapons expertise.

In addition, the Department and the nation should address all “low hanging fruit,” *e.g.*, eliminate the dominant radiological dispersal device (RDD) threat from the use of cesium-137 in blood irradiators, research irradiators, and calibration irradiators (Figure 6). Over 1,000 such sources, with 1,000 Ci or greater, exist in the United States today. Violation of any one of these sources could shut down 25 square kilometers anywhere in the United States for 40 or more years. An investment of \$200 million over a five-year period to buy up the Cs-137 machines and replace them with e-beam irradiators or cobalt sources would eliminate the most dangerous domestic RDD threat. This study urges the Assistant Secretary for Homeland Defense to lead DOD advocacy to replace these devices.



**Figure 6. Low Hanging Fruit: Eliminating the Dominant RDD Threat**

The recommendations presented here for nuclear, biological, cyber warfare, and other modalities are not a panacea and do not totally eliminate the threats. However, by implementing these recommendations the potential consequences of attacks from these modalities can be lowered significantly and can be made far less attractive to the adversary (Figure 7). Both are important to reducing the risk to the country, either directly or through the increased degree of deterrence that may be established.

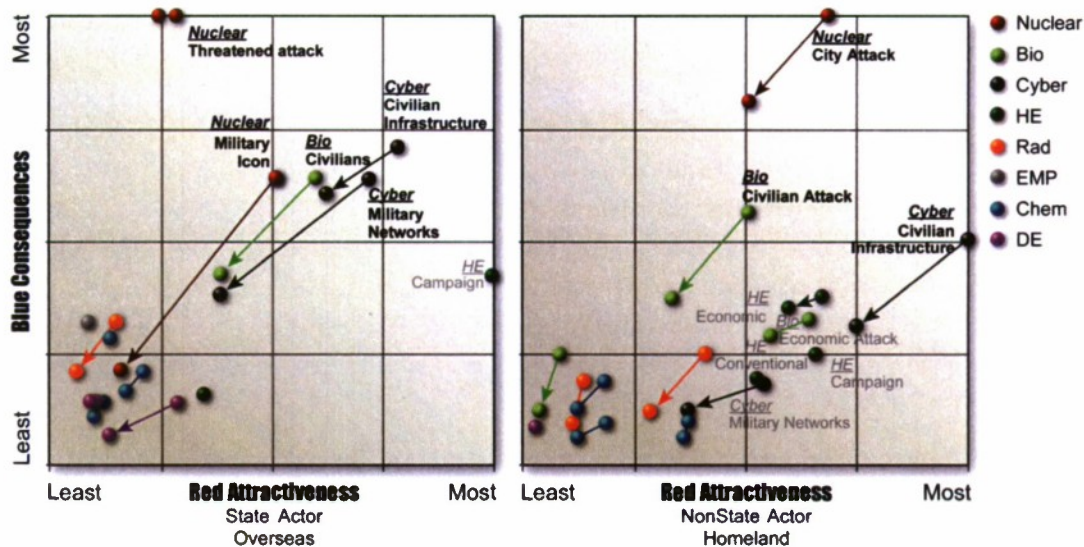


Figure 7. Red-Blue Perspective: After Recommendations

## Nuclear Proliferation: A Special Case

The previous section, which provided a broad overview of the technology landscape, illustrated the ways in which nuclear, cyber, and biological threats are separate and apart from the host of other problems in the emerging military landscape. That overview identified actions the nation should take to best position itself, should an attack using one of these modalities occur. In the case of the nuclear threat, recommendations focus on improving capabilities for attribution and consequence management. But, as was established in this assessment, and in previous ones by the DSB, the nuclear threat stands in a class by itself in terms of its potential for damage, disruption, and devastation. Thus, the matter of prevention—of managing the challenge of nuclear proliferation—deserves special attention.

### *Trends*

The proliferation of nuclear weapons to a larger number of states is proceeding. The exact form it will take over the next two decades cannot be known at this time. Yet there are strong views over the course it might take. Some believe that proliferation is inevitable—that the historical pattern of weapon acquisition every few years implies that this is so. By this view, the temptation to throw in the towel on proliferation prevention is strong but not sound. Another view suggests that the cascade is imminent—that the world is at another tipping point and spillover effects in several regions (North Korea and Iran) are inevitable with the potential for 20 or 30 nuclear-armed states in a decade or two. If this latter vision were to be realized, the world would be changed profoundly, and for the worse, by nuclear proliferation

While the world may well stand at another tipping point, a cascade of proliferation is not inevitable. History has shown that not every state that starts out wanting nuclear weapons ends up acquiring them (Figure 8). States make many decisions regarding the acquisition of nuclear capabilities and these decision points offer opportunities to influence the outcome. Many states have been persuaded to exercise restraint. Some of these states were U.S. friends and allies, who were persuaded with security guarantees. Others were less friendly, and they were persuaded by sanctions, threats, and other means. Regime change has been helpful too, among many other factors. But these experiences suggest that it is not necessary to accept proliferation as inevitable. What should be done in anticipation of more nuclear proliferation? What more can be done to prevent such proliferation?

As a starting point, this study identified four alternative proliferation futures, based on how trends evident from the first 60 years of the nuclear era might manifest themselves in the next 20 years.

1. **More latency.** In this future, there will be more states with weapons potential, more advanced weapons potential, and increasing risks of short cuts. Technology diffusion will accelerate, as will risks of smuggling and terrorist access.
2. **More minimum deterrents.** This future builds on the previous one, plus a few more states cross into production for the purpose of minimum deterrence.



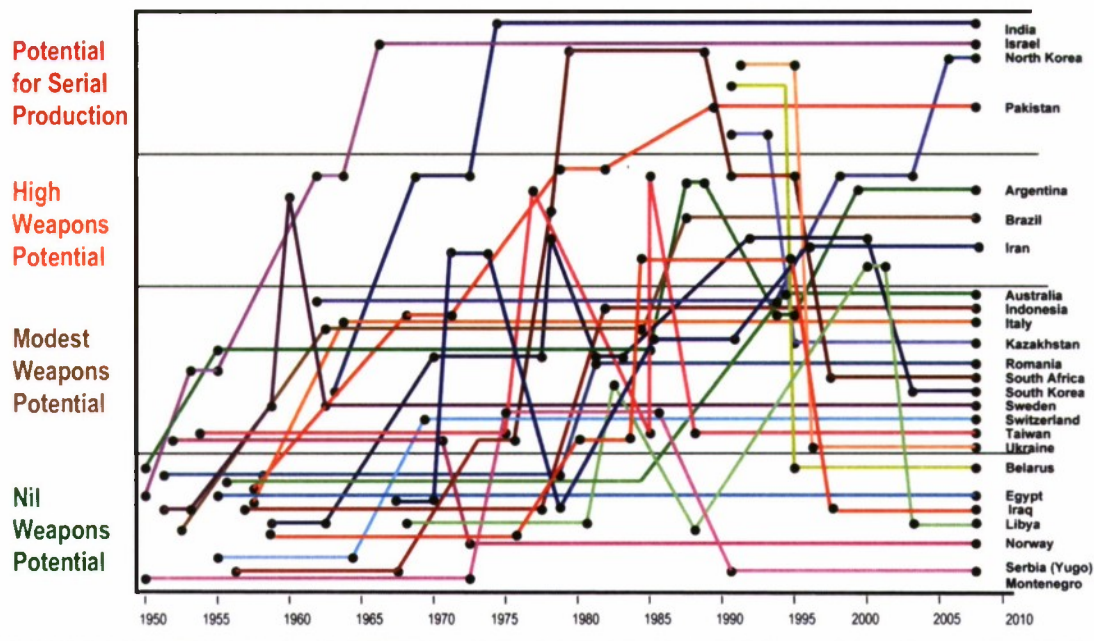


Figure 8. Of 24 Aspirants, Only Four Have Weapons Today

3. **New nuclear competition.** This future adds intensifying competitions within and among regions and, in a few cases, with the United States.
4. **New anarchy.** This future is separate and apart from the three above. While not a case of hyper-proliferation, in this alternative a nuclear revolutionary emerges who is willing to employ and share nuclear weapons.

Considering alternative futures is useful as it illuminates the demands that nuclear proliferation will impose on the U.S. military. It bounds the plausible problem space within which military operational challenges could arise and, in turn, points to needed military capabilities.

### *Needed Military Capabilities*

The toolkit needed to cope with the military operational challenges of a more proliferated world is large and diverse. It includes three basic types of capabilities. First, a joint force that is able to execute the missions associated with combating nuclear proliferation. Second, a strategic posture that is able to meet the demands of assurance, dissuasion, deterrence, and defeat. The third is the capacity to integrate all tools of national power.



The joint force must be able to perform the following missions effectively:

- **Interdiction** to locate and seize nuclear materials and weapons in transit
- **Elimination** to eliminate weapons captured from terrorists or collapsing or defeated states and the programs that produced them
- **Attribution** to provide a national assessment to the U.S. President within 24 hours of an unclaimed nuclear explosion and an international technical assessment to the United Nations Security Council shortly thereafter (within 120 hours)
- **Passive defense** to allow sustained operations in a nuclear contaminated environment (though not under sustained nuclear attack)
- **Consequence management** to prepare and protect civilian populations in affected areas
- **Intelligence** to provide timely access by the President of the United States, Secretary of Defense, and combatant commands to comprehensive, technically informed, actionable nuclear intelligence to support crisis action, network suppression, and longer-term planning

The strategic posture must be able to meet the demands of assurance, dissuasion, deterrence, and defeat with the following capabilities:

- **Non-nuclear kinetic strike** to hold at risk enemy nuclear assets and other high-value targets by non-nuclear means
- **Active defense** to defeat enemy preemptive or retaliatory strikes with active defenses
- **C4ISR** to find and track mobile systems, coordinate complex high-speed operations, and provide prompt situational awareness
- **Nuclear** to deter nuclear attack on the U.S. homeland and extend deterrence to allies and friends that they deem credible by nuclear and other means
- **Stewardship** to demonstrate high standards of responsible nuclear ownership
- **Infrastructure capacity** to respond to geopolitical change, technology surprise, and new mission requirements with new capabilities from a responsive infrastructure.

The third basic capability is the capacity to comprehensively integrate the tools of national power—diplomatic, information, military, and economic—across all phases of operations. Without such integration, the military will be called upon to do things that it is ill-equipped to do alone. Such integration is also essential for all of the Phase Zero activities (shaping operations aimed at conflict prevention) associated with proliferation prevention, assurance, and extended deterrence.

### *Assessing Current Capabilities*

In the assessment of this study, the gaps between current capabilities and future needs are large. Today's joint force lacks the necessary robustness to deal with plausible emerging threats in the nuclear arena. An evaluation of current investments to combat weapons of mass destruction shows that the vast majority of spending is for passive defense against chemical and biological attack, threat reduction cooperation, and missile defense. Spending on nuclear programs, within this portfolio, represents roughly 10 percent of the total. This investment seems too small and ill-balanced to generate major capability increases. But it is just enough effort to create the impression that enough effort is underway. In fact, the current level of effort is not consistent with the requirements of current national strategy, which makes it a priority now to be able to confront proliferators, dissuade their capability development, and extend deterrence and assurance to allies and friends.

Furthermore, the institutional capacity to deliver needed capabilities is underdeveloped. Over the past two decades, in which proliferation has emerged as a military planning problem, there has been much top-level guidance, but strikingly little progress in closing capability gaps. Part of the problem is that institutions that should guide the development of future capabilities seem ill-suited to the purpose. Three problems seem to dominate:

1. OSD is not able to direct resources effectively.
2. Capability-based planning is slow to deliver on this problem.
3. Improved intelligence outputs require much improved collaboration between intelligence and military communities.

### *More Effective Proliferation Prevention*

Actions can be taken by multiple actors in the defense community to accelerate capability and capacity development. In the view of this study, two objectives need to be met. The first is to accelerate the development of needed technical

capabilities by increasing the overall level of effort. Second is to enhance DOD's institutional capacity to advance capability and capacity development. Toward enhancing institutional capacity, the following recommendations are offered.

#### RECOMMENDATIONS: INSTITUTIONAL CAPACITY

USD (AT&L) designate portfolio managers for combating WMD and New Triad<sup>2</sup>; stand-up needed analytical capability.

USD (P) recreate a focal point for combating WMD at a more senior level (currently this is one issue in a very broad assistant secretary portfolio) and restore needed staff capabilities.

Joint Staff address misalignment of functional capability boards (force protection is too narrow).

Joint Staff get the front end of concept development right by completing the Joint Integrating Concept on Combating WMD and Joint Operating Concept on Shaping in ways that address proliferation requirements.

DTRA and Defense Intelligence Agency partner with National Counterproliferation Center to accelerate "over the horizon" analysis; complete five in two years.

U.S. Strategic Command Center for Combating WMD exercise one combatant command war plan with intelligence denied; assess how operations at all phases will be influenced.

If successfully implemented, these recommendations should help to ensure that nuclear weapons will not be embraced by enemies of the United States as their premier asymmetric capability.

Beyond these steps, more can be done to support proliferation prevention. A clear view of the past reveals that tipping points have been encountered before—in the 1960s and again in the late 1970s and 1980s. Although many experts anticipated a rapid spread of nuclear weapons in those periods, actual proliferation was far more modest. It proved possible to persuade most states to accept

---

2. The 2002 Nuclear Posture Review unveiled a new strategic triad, consisting of nuclear and precision non-nuclear strike forces; passive and active defenses; and a revitalized defense infrastructure.

alternative solutions to their security problems, such as security guarantees from the United States, or to accept a level of capability well short of actual weapons production potential.

Despite the stubborn character of the proliferation problems in North Korea and Iran, the participants in this study are hopeful that the present tipping point can again be managed in such a way as to minimize repercussions among their neighbors and beyond their subregions. This will again require sustained U.S. policy engagement and innovation employing the tools of deterrence and the treaty regime. It will also require that DOD develop tailored approaches to proliferation prevention for Combatant Command Phase Zero activities and that DOD work to energize an interagency process on these issues.

#### RECOMMENDATIONS: PROLIFERATION PREVENTION

**With USD (P) in the lead, DOD should develop tailored approaches to proliferation prevention that span the full problem space and work to energize an interagency process on these issues:**

- Compose country campaign plans
- Ensure participation of needed interagency partners
- Integrate into planning for theater security cooperation and Concept of Operations Plan (CONPLAN) 8099 Phase Zero
- Execute, assess, and adapt as theater security cooperation and CONPLAN cycles and circumstances require
- Develop capabilities and capacities that underwrite policy and strategy

---

Will nuclear proliferation endow a new tier of states with peer-like capabilities to limit U.S. freedom of action? Possibly. But whether this proves to be so is largely up to the United States. There is much that the nation can do militarily and otherwise to reduce the leverage others might gain with nuclear weapons and to shape their incentives and capabilities to acquire, threaten, and employ them. In the end, leadership matters. The United States must stay engaged in the effort to prevent proliferation and DOD must stay engaged in the U.S. effort. The recommendations offered here highlight the most important opportunities for doing so at this time.



## Unconventional Operational Concepts and the Homeland

---

The capable adversary of the future will execute “one game”—attacking U.S. interests wherever the nation is most vulnerable, and that could mean the homeland. When a determined adversary succeeds in attacking the homeland at the scale imagined in this study, the nation will call on DOD to “provide for the common defense” through both defense at home and offense abroad. DOD has, in fact, acknowledged such a future in its *2005 Strategy for Homeland Defense*, which states unequivocally that DOD must be prepared to defend the homeland:

The Department of Defense must change its conceptual approach to homeland defense. The Department can no longer think in terms of the “home” game and the “away” game. There is only one game. ... Defending the US homeland—our people, property, and freedom—is our most fundamental duty. Failure is not an option.

How well has the department progressed in turning that strategy into reality? This can be broken into three more specific questions as follows:

- How well do DOD and others understand what’s expected of them? How well prepared is DOD to execute across a range of homeland defense missions?
- Given the “one game” nature of the capable adversary, can DOD have high confidence that it will be able to ensure deployment and supply in whatever set of missions it undertakes, within and from the homeland?
- Success, in both the current scope of homeland security and defense and the more stressing environment of the future, depends on teaming and integration unprecedented in recent history: across and among all levels of government, with and across the private sector, as well as individual actions for preparedness. Where does the nation, and especially DOD, stand in building the “one team” needed for success?

### *DOD Roles and Responsibilities*

Overseas deployment, simultaneous with responding to a significant scale of attacks in the homeland, will stress DOD capabilities. The public expects that DOD will defend the homeland. DOD will be ordered to participate in homeland incident prevention, mitigation, and remediation through the U.S. domestic political process, regardless of the intentions of pre-incident military leadership. Legislation and directives support this approach.

However, at the next level, many responsibilities and missions are not so clearly acknowledged within DOD, resulting in the application of inadequate resources to the homeland defense mission. The problem extends beyond DOD to the interagency and response communities, where the handoffs and roles are not well understood—in part because they are not effectively exercised.

### **Scope of Roles and Responsibilities**

Defending the homeland includes a range of activities, most often discussed in terms of support to the civil authorities. But these activities can also progress to include a leadership role in response and consequence management efforts if or when the scope of an attack is severe enough. Even in a more limited support role, DOD leadership, both civilian and military, has been slow to accept this apparently expanded scope of responsibilities. A principle reason is that these responsibilities come with significant resource demands and financial costs that are not likely to be adequately supported. As a result, the resources and capabilities that DOD has to offer have not yet been effectively applied. DOD does not really know what is expected of it and the homeland security community does not know what to expect from DOD. The transition of responsibility across the various supporting and leading roles—and the handing off of these roles from one agency to another—are not well understood among the interagency and response communities.

A focus on specifics helps to better assess progress and gaps—the approach taken in this study. Reasonable roles for DOD in homeland defense include sharing intelligence, sharing infrastructure assurance standards (to support their mission), sharing operational doctrine and training, and providing consequence management support in case of an isolated terrorist attack or a natural disaster, such as Hurricane Katrina. Clearly DOD has lead responsibility for defense against air, missile, and maritime (with the Coast Guard) attack and for protection of its bases. DOD is in a lead role to assure the protection and resiliency of the defense industrial base, but it also must take a strong supporting role to assure protection and resiliency of other infrastructure that supports its missions (at least until a first significant attack(s) where it may be called upon to assume the lead). Roles that are not appropriate for DOD include protection of the country from internal threats like isolated terrorist attacks, production of WMD, or border monitoring for smuggling or illegal immigration.

To assure seamlessness among response elements and DOD, the Department must expand its concept of “jointness” to include other federal, state, regional, local, and tribal entities. This can best happen through leadership

and practice. But homeland security and defense leaders, both within DOD and other agencies, need to be developed, just as DOD has so carefully developed its leaders for the "away game." Planning, exercises, and training have yet to be conducted among all actors at all levels in any meaningful way.

### **Force Capabilities and Capacities**

The study's assessment of DOD's capabilities to execute its homeland defense roles is not a positive one (Figure 9). In the more traditional roles of air defense, missile defense, and maritime defense, DOD has or is developing a capability for these roles, but is far from having a well-exercised national set of capabilities. For example, while DOD maintains the best air superiority force in the world, its capabilities are not well suited to protect the nation from general aviation or unmanned aerial vehicle threats. Protection of DOD installations has been a focus of force protection programs for some time, but addressing cyber threats and WMD remain major shortfalls. In too many other cases, DOD preparedness falls woefully short. Combatant commanders, especially U.S. Northern Command, have made many of these capability requirements known, but priorities within the Department have placed resources elsewhere.

The situation is even more serious when the panel looked into force capacities that might be required to deal with a major event or adversary campaign in the homeland while also prosecuting offensive actions abroad. This dual mission alone infers a change in the estimates of total force requirements, and only worsens when the "double counting" of the reserve component, who might also be first responders, is added to the equation. As a benchmark, ~80,000 troops were deployed in response to Hurricane Katrina, a large fraction of which were National Guardsmen. Another 33 percent of the guard was deployed simultaneously in Iraq. Further, the National Guard is counted on to support their states, other states through mutual aid agreements, and to meet federal requirements.

Assessment of DOD Status	Expertise	Think They Have Role	Has a Plan	Has Necessary Capability	Exercised and Ready	How Good
Ballistic Missiles		LEAD				↑
Cruise Missiles		LEAD				
Aircraft/UAS		CO-LEAD		NCR Emphasis		↑
Maritime		CO-LEAD				↑
Conv. Explosive (IED)						
• Road/Rail		No				
• Market-School		No				
• Critical Infrastructure		No				↑
• DOD Installation						↑
• Defense Industrial Base						
Cyber Attack						
• Commercial Target		No				
• Critical Infrastructure		No				
• DOD Installation						
• Defense Industrial Base						
Combating WMD						

Figure 9. DOD Capabilities for Homeland Defense

Currently there is no ability to track the “double counting” or the “day job” skills of guardsmen and reservists. Many are first responders. Many have critical skills from their civilian jobs that would be useful in consequence management—skills such as telecommunications and utilities. Databases with such information could help tremendously in understanding how scarce assets are being allocated or help to identify the personnel with the best skill sets in response to emergency needs.

#### RECOMMENDATION: DOD FORCES AND CAPABILITIES FOR HOMELAND DEFENSE

Addressing the shortfalls will require significant resources, sustained commitment, and greater involvement with other agencies, especially the Department of Homeland Security. As first steps:

The Secretary of Defense should task the Assistant Secretary of Defense for Homeland Defense and America’s Security Affairs (ASD [HD&ASA]) to revise and implement DOD policies and procedures covering homeland defense requirements.



This tasking should include clarifying relationships, roles, and missions of all elements of homeland defense (federal agencies, civilian and private sectors, state and local responders, law enforcement, and others). This information would go far to eliminate the uncertainty and/or confusion about what is expected of DOD and what others can indeed expect of DOD. The scope should expand to include the contingency where DOD assumes the lead response role in the homeland. Only those policies and procedures that lower the barriers to planning, exercising, information sharing, cooperation, and coordination across the entire homeland defense community should be approved.

**Service Chiefs and the National Guard Bureau assess force requirement and adjust/adapt/expand force structure to meet the “one game” demands of the future.**

Force structure should be built not just to support the regional command war plans for overseas contingencies, but also for those being developed by U.S. Northern Command. The effort will involve the development of accurate databases to understand the civilian skills and job commitments of the reserve components in order to assess and address the “double counting” issue. It will also require close planning and coordination with the service secretaries across the doctrine, organization, training, materiel, leadership, personnel, and facilities spectrum in order to ensure that shortfalls are addressed.

---

### *Assuring Deployment and Supply*

This study considered two critical warfighting aspects occurring simultaneously in the homeland: defending against domestic catastrophe and ensuring deployment and supply. Domestic catastrophes can occur in an environment of large, undisciplined populations, which, can result in the destabilizing effect of violent attacks on society. On the other hand, military deployment and supply take place in a disciplined organization, trained to accomplish the mission. Yet the two are linked—military deployment and supply is critically dependent on infrastructure elements that may be destroyed or severely compromised in a domestic catastrophe. Three areas seemed most important for DOD attention: (1) critical infrastructure protection and/or resiliency, (2) logistics, and (3) family and individual preparedness. A fourth area, military installation protection and preparedness, was the subject of a recent DSB task force.

### Critical Infrastructure

DOD has responsibility for not only the protection and assurance of its own military installations and facilities, but it is also the lead agency for assuring the protection and resiliency of the defense industrial base infrastructure sector. In addition, DOD has a supporting role for 14 other critical infrastructures/key resources: transportation; information technology; telecommunications; energy; chemical; commercial nuclear reactors, materials, and waste; government facilities; emergency services; public health and healthcare; drinking water and water treatment systems; dams; postal and shipping; food and agriculture; and national monuments and icons.

DOD is starting to make progress in identifying what is critical through the leadership of ASD (HD&ASA)/Defense Critical Infrastructure Program (DCIP), supported by the Naval Systems Warfare Center in Dahlgren, Virginia. Together with the combatant commanders, they have developed and are implementing a “mission assurance” process that incorporates many of the recommendations of a prior DSB study regarding risk management and mitigation.<sup>3</sup> The process focuses first on identifying critical functions and capabilities—command and control; ballistic missile defense; intelligence, surveillance, and reconnaissance; and power projection, for example. This step is followed by identification and assessment of those few assets or facilities necessary to ensure the functions or capabilities.

The process also provides guidance to assess a number of critical infrastructures “outside the fence” on which DOD might depend and/ or need to defend. The (classified) list of mission-critical assets appeared logical, but not complete or consistent in the application of the criteria against which criticality was judged. Further, it does not capture cascading effects and infrastructure interdependencies. Recognizing that it is still a process getting started, this study concludes that more effort must be applied to get it right and complete. The biggest gap, however, is that no one is charged with the responsibility or authority to ensure that corrective actions are taken.

Despite nearly six years since September 11, 2001, many U.S. critical infrastructures remain vulnerable. For the DOD, many critical supply chains—meals ready to eat, missiles, munitions, and fuel, for example—are not as resilient as they should be. Critical infrastructure and sources of supply are owned largely

---

3. Defense Science Board Task Force on *Critical Homeland Infrastructure Protection*, January 2007.

by the private sector—security and assurance is their responsibility, which is monitored by other parts of the government.

DHS has the broader mission to lead infrastructure protection across all the agencies and sectors involved. While DHS has led the interagency and the private sector councils in developing a risk-based protection approach, so much remains to be done that it is not possible to say with confidence that the nation's infrastructure vulnerabilities have been adequately addressed. In general, the department lacks the regulatory or legislated clout to direct the private sector to consistent levels of security and/or resiliency.

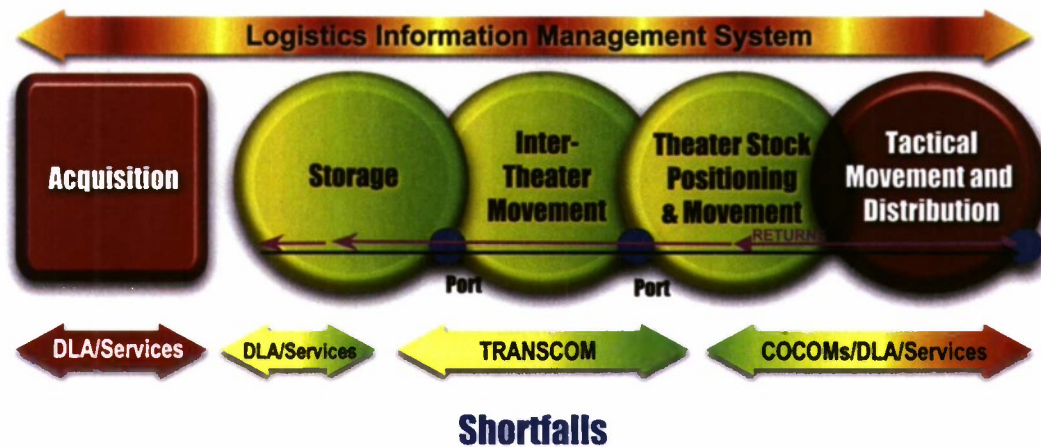
DHS has, however, done a good job at leading the national planning and grant processes, as well as overseeing lead agency activities with their sectors, in order to spotlight progress and gaps. At this point, DHS has identified 36 highest priority infrastructure assets and over 2,500 next level assets on which to focus attention, and, where appropriate, investment—under the constraint that much of the infrastructure is owned privately and therefore not eligible for public funds.

Of particular concern, however, is the difficult job of information assurance. There appears to be no national improvement plan in spite of countless admonitions to, and within, the government that such a plan and its implementation is a must. An important consideration for each federal sector owner is the fact that improvements in resiliency of the infrastructure will come about largely by its private owners. Developing a public-private partnership is no more important than in this area, and some attention to incentives to the private sector for improving its posture is warranted.

### **Logistics**

The study was pleased to learn that a number of the problems plaguing the DOD logistics community for years appear on their way to being solved—at least those within the domains of the Defense Logistics Agency (DLA) and U.S. Transportation Command. Enabled by the introduction of modern information systems, the two agencies are now able to understand inventories in their depots, and track supplies in transit to the warfighter and their delivery to transfer points to the services (Figure 10). Redundancy and/or alternatives exist for movement of supplies within and out of the United States.





**Figure 10.** Progress in Integrated Logistics, but Still Many Shortfalls

The weak links in the system are at the start and end points, with respect to the information system “glue” that integrates it end-to-end. Strategies are not yet developed to assure the availability of materials from the private sector within the homeland and of transportation routes required for their delivery from industry to DOD facilities in the event of attacks on the homeland. In addition, many spare parts for critical weapon systems are produced either by sole source companies or by companies with limited competition. Protection of critical sources of supply has not been planned. Diversion of supplies and materiel to civil priorities has also not been planned as a contingency in the event of major incidents at home.

On the other end of the supply chain, there has not been a coordinated effort to implement a single asset visibility system for the “last tactical mile” that would allow for tracking and reporting consumption to the DOD national provider or the end-user. The visibility inherent in the upstream steps is, at this point, lost, so that the individual requestor often does not see what has been ordered in a timely fashion, or sometimes not at all.

Cross-cutting the entire enterprise is the information management system. DLA is paying considerable attention to its network defense, but has further to go in addressing a wider spectrum of cyber threats.



### **Military Installation Protection**

In addition to ensuring that DOD can get material for warfighters from a robust private supply and internal distribution system, DOD must also assure the security of the forces it expects to deploy. The first step is assuring the inherent security of the installation itself. Each of the military services approaches base security and force protection differently, but almost all of them plan on the support of the local community emergency response resources in a serious incident.

For example, in the Army, mission commanders establish what is mission-critical. All garrison commanders have memoranda of understanding with the local community for first response capabilities. Both garrison and mission commanders coordinate plans for deployment under catastrophic scenarios. Annual exercises and training test commanders' ability to respond to incidents.

The civilian capabilities, on which military installations rely, will not be available if the incident is an attack of a serious scale, such as an attack using weapons of mass destruction—a particular concern of this study. Consequence management is the biggest gap in dealing with weapons of mass destruction. Project Guardian provides basic response capabilities to installations—chemical, biological, radiological, and nuclear—but is not scoped for anything of major consequences to the installation or surrounding community.

The DSB Task Force on Critical Homeland Infrastructure Protection assessed best practices for protecting U.S. homeland installations and recommended various approaches to enhance security and protection of these facilities. This task force determined that DOD has many facilities that are vulnerable to the threats considered in this study, but that a rational focus should be on protecting its critical military mission capabilities and functions. It also found that the degree to which DOD facilities are dependent on non-DOD infrastructure is not entirely known. Further, until recently DOD lacked policies and standards to guide installation commanders in securing or creating contingencies around the infrastructure on which they depend.

The critical infrastructure protection task force made many recommendations to improve DOD capabilities. This summer study agrees with and endorses those recommendations and, as a result, did not revisit the issue in its deliberations. But through information gathering related to installation risk assessments and management, the study believes that while progress is being

made, resources remain limited and priority remains highly dependent on the installation commander.

### **Family and Individual Preparedness**

There are many examples where individual preparedness proved pivotal in mitigating the consequences of a natural disaster (Florida's resiliency to numerous hurricanes since Hurricane Andrew versus Louisiana's response to Hurricane Katrina), and also how strong a role it played in the early days of the Cold War. In the event of coordinated asymmetric attacks in many parts of the country and/or simultaneously with a natural disaster or avian flu pandemic, emergency responders and relief organizations may not be able to move across local or state borders. Resources will be severely strained and responders will be busy dealing with or preparing to deal with disaster on their home turf.

The situation with military families deserves special attention. DOD must recognize that soldiers, sailors, airmen, and Marines will not likely be effective warfighters if they are simultaneously worried about the security of their families. While obvious steps, such as increased base protection, can be implemented, too many families live outside the installation. Instilling and promoting a culture of preparedness can provide both physical and psychological benefits to members and their families. There is much that can be done without great expense or effort to better prepare for both natural and man-made disasters.<sup>4</sup> Greater hazard awareness, training, home storage, and family communication/evacuation plans can provide greater peace of mind, strengthen mental resiliency, and empower DOD families to carry on through a disaster. Preparedness also reduces the impact of a crisis and likelihood that these families will have to depend only upon the emergency relief infrastructure. Self-sufficiency also empowers members and families to help others and set an example the community can follow.

---

4. Events include such things as floods, mudslides, hurricanes, tornados, fires, severe snow or ice storms, earthquakes, volcanoes, infectious disease outbreaks, severe power and fuel outages, hazardous chemical releases, nuclear or radiological incidents, and acts of terrorism and/or civil disturbance.

### RECOMMENDATION: ENSURING DEPLOYMENT AND SUPPLY

Recommendations in this section are limited to those that affect DOD, although there are many related items that DHS should address, as well.

**To better ensure deployment and supply, the Secretary of Defense should direct:**

- ASD (HD&ASA)/DCIP to extend the mission assurance process to the defense industrial base and recommend approaches for addressing shortfalls
- USD (AT&L) to work with defense industrial base owners to develop and implement corrective action plans
- ASD (HD&ASA)/DCIP to develop a prioritized action plan for addressing identified risks to DOD-owned assets
- U.S. Northern Command to lead implementation of actions identified by ASD(HD&ASA)/DCIP for critical function assurance
- Service secretaries to fund actions for mission assurance in owned functions
- Deputy Under Secretary of Defense for Logistics and Materiel Readiness to ensure resourcing of logistics shortfalls:
  - to assure sources of supply and movement to DOD depots
  - to eliminate the last tactical mile issues
  - to make the information management system interoperable, robust, and resilient to attack, from both within and outside

**Service Chiefs should actively promote the ability of military families to shelter at home for two weeks, or evacuate on short notice. They should:**

- Reinforce the message via noncommissioned officer leadership academies, on-base medical community, Armed Forces Network, unit town-hall meetings, movie/TV celebrities, veterans organizations
  - Assure base commanders export this capability to adjacent civilian communities.
-

### ***Building the National Team.***

The third dimension of this assessment of homeland defense addressed the status of the “national team” and DOD’s involvement. This is not a good news story. Homeland security organizations responsible for dealing with national calamities are a diverse lot: federal agencies, state and local authorities, and private firms. DHS, as the lead agency for creating that level of response, is still in its infancy. At the state and local level, there appears to be little that is positive about the relationship with federal “partners.”

DHS continues to reorganize, changes points of contact frequently, and brings to the table too much of a “we’re in charge” attitude. This judgment is shared by the private sector, although DOD’s relationship with the defense industrial base seems to be better than between many other sectors and their federal agency lead. U.S. Northern Command, DOD’s principal operating “face” to the homeland security community, has been restrained by DOD leadership’s view that the priority is—and should be—the “away game.” Its low profile start has produced serious perception problems that must be overcome among the partners with whom it will be called upon to work.

### **The Team Members and Relationships**

**Interagency.** In the interagency arena, a positive example of how things should work can be found in the Joint Interagency Task Force – South.<sup>5</sup> This pairing of military and civilian government agencies under a unified command structure provides for routine interaction between the entities that will need to work together effectively during a crisis. The DSB believes that the complex network of interdependent roles, responsibilities, and relationships demands a full-time integrated approach to homeland security and homeland defense activities through a number of similar standing operational task forces.

**Federal-State-Local.** In the case of a point attack, the first manifestation—and response—will occur locally. If or when those resources are overwhelmed, requests to the state will be made, and the governor can call out the National

---

5. Joint Interagency Task Force – South has the mission of monitoring and interdiction of illicit trafficking from Latin America. Membership includes Customs and Border Patrol, Central Intelligence Agency, Drug Enforcement Agency, Department of Defense, Defense Intelligence Agency, Federal Bureau of Investigation, Immigration and Customs Enforcement, National Security Agency, and the National Geospatial Agency.



Guard, as well as exercise mutual aid agreements with other states for additional response resources. When those avenues of response are tapped out, appeals for federal help can and will be made. However, during its investigation, the study team heard from several state and regional response leaders that federal support can be slow in coming and what they can expect is largely unknown.

With respect to prevention, state and local response leaders noted how much they can contribute, provided they have adequate threat information on what they should be anticipating. In other words, a strong partnership with their federal counterparts can contribute significantly to threat mitigation and/or apprehension. Positive examples of preparation and monitoring for Y2K and state/local threat assessment centers bear out the power of such partnerships.

**Public-Private.** Possibly the most neglected member of the homeland security/defense team is the private sector. The private sector owns most of the infrastructure and will be the most effective in protecting (given timely and adequate threat information) and restoring its function after an attack. As such, it must be an integral member of the team alongside government actors in federal planning and information-sharing activities.

Relationships between sector owners and operators and their federal agency interfaces are uneven—a striking condition that emerged during the course of this study. In some cases, especially where there is a history of a non-regulatory partnership, like the defense industrial base and energy sectors, relationships were positive, characterized by open and frequent communication and information sharing. Others were more one-way, with the federal “partner” more controlling and didactic. The realization that the sectors have more intimate knowledge of not only their own sectors, but their ties to other sectors, has yet to be well understood and embraced at the federal level.

**Leadership.** Forming a truly joint homeland security and defense team starts with developing leaders with a joint perspective—both through education and career experiences—building an interagency cadre of leaders, whose understanding of homeland defense transcends their immediate position. Homeland security and defense, regardless of agency, level of government, or public or private sector, must be seen as a professional opportunity for those seeking to lead in this critical field. However, there is no recognition of the need to develop homeland security leadership in the same manner as the nation has invested in developing national security leadership.

### **Plans and Exercises**

While numerous doctrinal and operational plans exist, most with embedded processes for review and revision, there are no processes to ensure that the plans are practiced and capabilities measured against readiness metrics. While there are many exercises (possibly too many), the exercises are highly scripted, unconnected to each other, and typically focus on a top-down approach (where the supporting organizations are “training aids” to the senior-level players) instead of bottom-up approach (focusing on an integrated and layered response beginning with the initial event). Even the national level exercises have not been effective—more often broad than deep, where the real lessons get learned. Furthermore, these exercises often stop before the more difficult issues—transfer of command, employment of specialized assets, or unknowns such as public panic—come into play. Even more worrisome than the disjointed nature of the exercises is the lack of any process for effectively “learning from” the lessons of these exercises. This gap extends to DOD, where the numerous exercise programs do not appear to be effectively linked to national objectives.

### **Crisis Communications**

Communications is almost always at the top of the list of recurring issues in a crisis. It can make or break a successful response. It starts with the basics of compatible equipment and language among response communities. It extends to the public-private linkage, where both the pre-emptive and response actions by private sector owners of critical infrastructure can mitigate significant problems, yet they are, more often than not, kept in the dark or not allowed access. (This was an acute problem in recovery and restoration post-Katrina.) It covers also communications to the public. Too often it is developed “real time” without benefit of factual vetting and without coordination, such that what is communicated to the public can be misleading or just outright wrong (as example, the anthrax attacks in 2001). The DSB believes that if there is only one thing that DHS and DOD ought to improve among the national team, it should be crisis communication.

## **RECOMMENDATION: BUILDING A NATIONAL TEAM FOR HOMELAND DEFENSE**

Secretary of Defense leadership in the interagency is needed to address current deficiencies in national plans and strategies and support for domestic threat assessment. DOD needs to step up to its preparedness responsibilities in the broad set of communications issues.

To address deficiencies in plans and communications, the Secretary of Defense should:

- Promote the combination of the National Security Council/Homeland Security Council to coordinate and integrate a national strategy and response for global asymmetric engagement
- Request a national intelligence estimate on the scope of the projected threat.
  - direct the Office of Net Assessment to conduct a capabilities-based net assessment
- Request that DHS work with DOD to codify the transition from DOD support to DOD lead for a war at home
- Direct the Deputy Secretary of Defense to develop a comprehensive DOD communication system and public affairs strategy for homeland defense preparedness and crisis/consequence management.
  - develop an equipment and concept of operations architecture compliant with the National Incident Management System
  - ensure availability of DOD communication assets compatible with civilian responder community
  - work with DHS to develop messages, and coordinate and educate those who deliver them, appropriate to the full range of contingencies

The Secretary of Defense should direct U.S. Northern Command to work with the National Exercise Program at DHS to design and execute more effective exercise programs that address:

- Unified management of national capabilities
- Communication and information sharing across public and private boundaries
- Regional planning and coordination
- Interoperable and response capability shortfalls
- Transition from DOD support to DOD lead scenarios

In the layered approach to DOD's Strategy for Homeland Defense and Civil Support, one of the layers—"Enable"—is directly focused on improving domestic capabilities through sharing DOD expertise and technology. The military is recognized for its unsurpassed training, exercise, and doctrinal programs.

**ASD (HD&ASA) should take the initiative to help establish a strategically-managed, interagency homeland defense/homeland security leader development program with the following attributes:**

- Graduate-level, senior service DHS-sponsored "war" college developed in conjunction with the National Defense University
  - An Executive Exchange Program modeled on the President's Executive Exchange Program
  - Recognition as credit equivalent to senior service schools and for flag/senior executive service promotions in DOD
  - Training expanded to state and local levels
- 

## **What We Know and Don't Know about Adversary Capabilities: Intelligence**

This study's "Know/Don't Know" analysis was designed to assess U.S. knowledge and gaps related to weapons of mass destruction, cyber, and high-leverage asymmetric threats—and, where gaps exist, to make recommendations for closing them. The "Know/Don't Know" formulation was used rather than a more conventional assessment of the nation's intelligence posture in order to ensure that the "Don't Knows," particularly at the levels of strategic threats, are unambiguously used by the Intelligence Community. To drive or compel response, actions in collection, analysis, and customer interaction are offered.

The study concluded that improvements are needed in number of areas: foreign intelligence collection, analysis, and customer support activities; domestic intelligence associated with foreign-inspired threats to the U.S. homeland; countering foreign intelligence; net assessments and gaming; and methods for improving intelligence related to the threat of weapons of mass destruction and other high-leverage adversary means.



### *Know/Don't Know Posture*

While much of the assessment of the community's know/don't know posture is classified, this study does concur with the sentiments of the 2005 WMD Commission, which asserted that "strategic issues" such as these should command top level focus in the Intelligence Community and, further, that the community should devote some of its best collection, analysis, and customer interactions to these topics.<sup>6</sup> Yet, two years later, it is still not clear that the community has internalized these observations, nor taken deliberate steps in the areas of collection, analysis, and customer support efforts to devote the necessary resources to strategic threats.

#### **RECOMMENDATION: KNOW/DON'T KNOW POSTURE**

To better position itself to close strategic information gaps, the intelligence community should create a set of X-treme intelligence teams, staffed with some of the community's top talent, to focus on a small number of hard problems.

### *Intelligence on Foreign-Inspired Domestic Threats*

Among the most stressing challenges to U.S. military operations are threats to homeland-based forces, operations, resources, and assets. Foreign-inspired domestic threats remain largely unknown to U.S. intelligence and, therefore, will present high-order challenges to U.S. military operations in future engagements.

DOD is responsible for force protection (and critical defense infrastructure on which it is dependent, including the industrial base) but does not have and cannot presently acquire sufficient understanding of the threat within the United States—adversary plans, intentions, and capabilities to disrupt or deny critical defense assets. The bottom line is that the nation does not have the intelligence it needs to protect mission-critical DOD activities at home. Moreover, DOD has not adequately defined its requirements for intelligence support at home.

U.S. intelligence lacks situational awareness and sophisticated understanding of foreign-inspired threats or operations within the United States. Intelligence on

---

6. *Final Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 2005.

foreign-inspired domestic threats must be derived in part from contributions of independent law enforcement agencies at the federal, state, and local level. But many of these organizations lack the training or established processes needed to function as intelligence producers. Without change, DHS, the Federal Bureau of Investigation, and other law enforcement organizations, along with the existing intelligence community entities, will not be able to provide adequate domestic intelligence to meet DOD mission needs.

In the course of its assessment, this study reviewed the model used by the New York City Police Department (NYPD) in dealing with this threat. The NYPD has adopted an approach for utilizing strong intelligence collection and analysis methodologies, which may be an ideal “franchise model” across localities critical to DOD missions.

#### **RECOMMENDATION: DOMESTIC INTELLIGENCE**

The Under Secretary of Defense for Policy, working with the Under Secretary of Defense for Intelligence (USD [I]), should ensure that DOD identifies military capabilities in localities where the New York Police Department model may be more aggressively applied.

The USD (I) should strengthen his role as the DOD focal point for intelligence in support of defending U.S. military homeland-based capabilities, assets, facilities, and functions.

---

### ***Countering Foreign Intelligence Threats***

Foreign intelligence operations against the United States are now more diffuse, more aggressive, more technologically sophisticated, and potentially more successful than ever before. In particular, the use of human intelligence operations by weaker powers to achieve advantage is a classic “asymmetric strategy,” which increasingly will challenge future U.S. military operations as adversaries learn from past successes. Given DOD’s global responsibilities, activities to identify, assess, and defeat foreign intelligence activities are an ongoing defense mission, spanning peacetime to wartime.

Today, defense counterintelligence is a collection of disaggregated and service-driven operational programs, each with distinct doctrinal and organizational bases that are grounded in history and the differences in service

missions. The Secretary of Defense does not have unity of command with respect to the counterintelligence forces that are assigned to identify, assess, and defeat these threats. Operational intelligence on foreign intelligence activities is poor. And while military service counterintelligence components provide support to individual combatant commanders, the command structure is ill-suited to undertake global operations against an adversary intelligence service. A genuine Goldwater-Nichols-like transformation is needed to create true joint operations with strategic-level focus.

#### **RECOMMENDATION: COUNTERING FOREIGN INTELLIGENCE**

**The Secretary of Defense should establish a joint operational component within DOD with the standing mission of detecting and degrading foreign intelligence capabilities that threaten U.S. military operations while retaining the focus of the service counterintelligence organizations.**

---

This new organization should be responsible for robust planning, developing doctrine, assigning resources, and directing and executing operations to achieve the mission of degrading foreign intelligence capabilities. This organization should galvanize intelligence community support for the defense counterintelligence effort and provide the nucleus for a serious national-level strategic capability.

#### ***Need for Strategic Analysis***

Net assessment (blue on red interaction) has proven itself in identifying important gaps in complex and multi-dimensional military problems. Given the poor state of knowledge of stressing wars in the future, net assessment, gaming, and simulation techniques should be employed to identify and understand intelligence gaps, the implications of those gaps, and commensurate intelligence opportunities. Employing such tools would also sensitize the blue side to the existence of such intelligence gaps.

### RECOMMENDATION: STRATEGIC ANALYSIS

**The Office of Net Assessment, USD (I), and the Director of National Intelligence should establish a capability to assess big complex peer problems (e.g., space anti-access) for net assessment and modeling of future stressing war.**

The recommendations described herein are targeted to improve U.S. intelligence capabilities in support of future stressing wars. The challenges ahead will require broad emphasis on counterintelligence, foreign-inspired domestic threats, and the other challenges described in this section. Many of these recommendations involve new ways of doing business, improved collaboration among community organizations, and attention from the community leadership to ensure adequate resources are directed to these efforts.

## Fighting Through Asymmetric Counterforce

The United States has plans to improve its conventional military capability that should enable our nation to retain its advantage in force-on-force capability through the next several decades. Faced with this conventional advantage, potential adversaries will likely seek asymmetric methods to undermine and ultimately deter or influence U.S. military operations. Such asymmetric methods might include attacks on U.S. vulnerabilities, the use of deception to avoid a direct U.S. response, use of non-attribution, and intimidation of allies. Such methods might be employed, for example, to attack command and control assets of deployed military forces, interrupt logistics lines of communication, or attack the U.S. homeland, as previously discussed.

Not only might adversaries employ such methods in single attacks, they may also seek to employ multiple asymmetric attacks that simultaneously impede or deter U.S. military operations in multiple locations abroad, or both abroad and at home. It is possible that an adversary may be sophisticated enough to optimize a series of asymmetric attacks that could cripple U.S. military operations and do so while maintaining anonymity. There are numerous potential combinations that planners must imagine and consider in order to prevent or counter an adversary's attempt to undermine U.S. military capabilities at home and abroad.



While the range of potential asymmetric attacks is wide, this study chose to focus its work on a small set of the most compelling challenges, selected based on the following criteria: (1) possible catastrophic effect on military operations, (2) adversaries will have the means to provide these challenge, and (3) DOD is not doing enough to prepare for dealing with them.

The three challenges are:

1. **Conducting military operations in WMD environments.** This challenge includes the threat of or actual use of WMD (biological, nuclear, chemical, radiological, and others) against U.S. forces and/or those of an ally. Countering this threat involves protecting critical bases of operations and projecting and sustaining forces in distant anti-access environments.
2. **Countering attacks on U.S. and allied space capabilities.** Critical to this challenge is gaining and maintaining space situational awareness, conducting defensive and offensive counter space operations, and conducting combat operations when space capabilities are degraded.
3. **Cyber warfare against information and networks.** The challenge of keeping pace with this ever-advancing threat is real. Counters include learning how to operate with degraded networks and corrupted information and developing integrated applications of cyber defense, attack, and exploitation.

The ability to operate in and from the global commons—space, international waters and airspace, and cyberspace—is critical to DOD's ability to conduct operations and project power anywhere in the world. The two domains of the global commons that are most at risk are space and cyberspace. Space is vulnerable because of new threats; cyber because an increased dependence on rapidly evolving information networks creates new vulnerabilities that adversaries are already seeking to exploit.

The future will likely bring an enlarged set of players, both state and non-state, with incentive and capability to use WMD, either to disrupt U.S. military operations or to intimidate or even attack their regional neighbors. To meet this challenge DOD will need to enhance U.S. capabilities to: (1) dissuade possession of WMD, (2) deter WMD attacks and threat of attacks, (3) disarm adversaries possessing WMD weapons, (4) enhance capabilities of general purpose military forces to operate in a WMD environment, and (5) mitigate the damage done by a WMD attack. Combat in a WMD environment is not the same as combating WMD. Thus, the focus of the recommendation herein is to enhance the capabilities of general-purpose forces to operate in a WMD environment—to fight through the asymmetric counterforce.

### *Fighting an Adversary Possessing WMD*

DOD needs to take steps to make its military operations less fragile to WMD attacks. This assertion, on the part of this study, is not meant to suggest that U.S. forces be prepared to operate against massive and protracted WMD attacks where U.S. retaliatory capabilities play a critical deterrent role. Rather, U.S. military operations should not be held hostage to limited WMD attacks that may not even be attributable. Three areas were emphasized in the study deliberations: building partnership capacity, preparedness to fight in WMD, and vulnerability to small-scale nuclear attacks.

#### **Building Partnership Capacity**

U.S. military operations depend on host nations for bases and logistics support, and on contractors, host nation populations, and other critical civilian personnel to deploy and sustain the force. For the most part, however, these elements lack the protection afforded U.S. forces from chemical, biological, and radiological attacks and, as well, lack the same capability to manage consequences—though they are subject to the effects of WMD attacks against U.S. forces. Host nations and supporting forces may be less willing to support U.S. military operations in the face of WMD threats if they perceive that they will suffer disproportionate losses. Loss of partner support could have catastrophic effects on the outcome of a conflict.

Helping partners prepare for and manage the consequences of WMD attacks is a key element in any strategic communication plan. The *2006 National Military Strategy to Combat WMD* states that, “[DOD] must assist international partners to build capacities to combat WMD effectively.” While DOD has made initial steps toward building partnership capacity, it is under-resourced and does not focus on fighting through WMD. Further, some current authorities—such as the prohibition of National Guard WMD Civil Support Teams to operate overseas—limit DOD’s ability to build partner capacity for WMD.

**RECOMMENDATION: BUILDING PARTNERSHIP CAPACITY TO FIGHT THROUGH WMD**

DOD should establish a discrete funding line of not less than \$500 million to enhance partners' capability to fight through WMD.

USD (P) should direct recurring and stable programmed funding of \$18 million per year for the National Guard State Partnership Program.

Secretary of Defense should request that Congress rescind the current statutory provision that prohibits the use of the National Guard Civil Support Teams.

---

**Preparedness to Fight in a WMD Environment**

U.S. forces routinely trained during the Cold War for operations in a WMD environment—fighting through chemical, biological, and even nuclear effects. Since the end of the Cold War, the WMD environment has changed, but concepts and doctrine have not kept pace. As a result, U.S. forces are better organized and equipped but not as well trained to fight in a WMD environment today. The demands of current operations have reduced the time that most forces are able to train for operations in a WMD environment. Exercises are infrequent and seldom continue past the point where WMD are used against U.S. forces. The exception, perhaps, is Korea, where the proximity of a major chemical threat motivates readiness.

Strategies and concepts that provide the framework for fighting in a WMD environment are incomplete and inconsistent. The “combating WMD” construct embodied in DOD directives and joint doctrine identifies the need to tailor capabilities and operations to perform in WMD environments. But implementation to date has emphasized interdiction and defeat of the weapons themselves, with little attention to the capabilities needed to fight in a military campaign against an adversary armed with and willing to use WMD.

In the absence of concepts and doctrine to drive capability-based assessments that would determine needs and identify gaps, U.S. forces may not be adequately prepared for fighting through the effects of WMD. This could result in U.S. forces suffering massive losses or even being rendered combat-ineffective in the event of such attack. Further, plans not validated through realistic exercises may be ineffective in the face of WMD attacks.

**RECOMMENDATION: PREPAREDNESS FOR COMBAT IN WMD**

The Joint Requirements Oversight Council should direct a series of capabilities-based assessments to identify capability needs and gaps for operating in a WMD environment.

Joint Forces command should conduct a series of experiments, with the support of U.S. Strategic Command's Center for Combating WMD, to explore WMD-related issues associated with operations in a WMD environment.

Chairman, Joint Chiefs of Staff, should direct the combatant commands to place particular emphasis on joint and multinational exercises where "fighting through WMD" is a main objective.

---

**Small-Scale Nuclear Attacks**

Given current methods of operation, forces overseas are vulnerable to the use of tactical nuclear weapons by adversaries who may not be deterred. Deployment and resupply capabilities force reliance on vulnerable, easily targeted nodes. Maritime forces are operating more in littorals but concepts of operation do not reflect their increased vulnerability in nuclear, biological, or chemical environments. Since the end of the Cold War, attention to hardening equipment against the threat of blast, thermal, and electromagnetic pulse effects has abated due to a combination of expense and pressures to cut costs. Command and control networks, which vary considerably from theater to theater, based on geography and availability of systems, are not subjected to nuclear vulnerability analysis that is essential to identifying potential single points of failure.

As mentioned previously, U.S. forces are better protected against chemical and even biological attacks than the civilians and foreign nationals on whom they depend. But nuclear attacks pose a much larger challenge. Even a single nuclear weapon could render key nodes unusable for extended periods, and electromagnetic pulse effects from a limited nuclear attack could blind sensors and shut down key command and control systems.



### RECOMMENDATION: SMALL-SCALE NUCLEAR ATTACKS

U.S. Strategic Command help combatant commands anticipate nuclear effects and plan to fight through them.

The Defense Information Systems Agency (DISA) develop tools for C4ISR network analysis to reduce critical node vulnerability, establish redundancy requirements, and identify options for degraded operations/reconstitution.

Secretary of Defense direct DISA and DTRA to assess utility of nuclear hardening techniques for critical network elements.

### *Countering Attacks on U.S. and Allied Space Capabilities*

U.S. military operations have become dependent on space assets to enable command and control; intelligence, surveillance, and reconnaissance (ISR); navigation; precision attacks; beyond line-of-site communications; and weather and environmental information. Adversaries are well aware of this dependency and are developing threats to these assets. For example, the Chinese conducted an anti-satellite test on January 11, 2007. Currently, the United States and its allies are not well-prepared to defend against such attacks as space has been long perceived as a peaceful sanctuary. But if critical space assets are not properly defended, the results may be catastrophic not only for the United States and its allies, but for the world economy as well. Thus, the nation must be prepared for both defensive and offensive counter-space operations.

Due to the dependency on space assets, a successful attack, would severely impact U.S. and allied military capabilities. Conducting joint warfighting operations in an environment where command and control, ISR, navigation, and communication and other systems are either degraded or denied would be extremely challenging at best. At worst, it could mean defeat for the United States and its allies. The effect on the global economy could be equally severe with telecommunications, transportation, and commercial navigation degraded as well as disruption of financial transactions. Moreover, political alliances, coalitions, and partnerships may be undermined if the United States is not well trained, equipped, and prepared to respond.

### Space Situational Awareness

The growing number of objects in space will make maintaining space situational awareness more challenging. In the late 1950s, there were only four objects in low earth orbit to track and catalog. In the last forty years, that picture has changed dramatically. Forty-four nations and several commercial enterprises have objects in space. Low earth orbit (LEO) and geosynchronous earth orbit (GEO) positions are becoming increasingly crowded. Tactical, mini, and nano satellites are now being launched by both government and commercial entities.

All together, the evolution in the use of space, which is expected to continue apace for decades to come, complicates the job of maintaining space situational awareness. Space debris is another problem as well. Government and commercial satellites have to be maneuvered to avoid collisions with other space objects. During such maneuvers, satellite services are normally suspended, consuming precious on-board fuel and interrupting operations.

The current space surveillance network is struggling to keep track of 11,000-plus cataloged objects (satellites and debris), a number that could grow dramatically over time, especially if satellites are physically destroyed by adversary attacks. The complexity of the situation in space can pose significant challenges for military operations. If DOD forces cannot assess, characterize, or attribute an attack to its source, then executing an effective response will be all but impossible.

#### RECOMMENDATION: SPACE SITUATIONAL AWARENESS

DOD needs to field an improved Space Surveillance Network that produces an automated single integrated space picture; incorporates southern hemisphere coverage and new sensor capabilities; and supports distributed, collaborative space command and control operations.

The services need to begin incorporating attack assessment/attack reporting sensors on key space assets.

USD (I) request the Director of National Intelligence to focus additional national intelligence resources on collecting and analyzing space intelligence.

---

## Space Control

The Department of Defense needs to take more seriously the prospect of conducting offensive and defensive operations in space and rapidly reconstituting space assets. Today the processes for determining post-attack response options are not well defined. The intellectual foundation—doctrine; concepts or operations; tactics, techniques, and procedures—dating back more than five years has not kept pace with changes in the security environment. Current joint exercises do not emphasize space control. In addition, tools or systems for countering attacks are insufficient.

### RECOMMENDATION: SPACE CONTROL

**USD (P)** articulate policy on protecting U.S. and allied space capabilities, including guidance on sharing space situational awareness information and coordinating response options.

**U.S. Strategic Command** develop joint space control doctrine; concepts of operations; and tactics, techniques, and procedures.

**Services** improve both defensive and offensive space control capabilities. Harden satellites, add attack detection sensors, improve ground station physical security, and add redundant and secure communication means.

**Develop** a rapid global strike capability.

**U.S. Joint Forces Command** incorporate realistic space threats and space control play into education, training, and exercise programs. Also upgrade information operations range to incorporate space range capabilities.

**U.S. Strategic Command** develop a responsive space reconstitution program.

## Operating in a Degraded Space Environment

U.S. forces need to be better prepared to conduct campaigns when space assets are degraded. The U.S. space architecture will remain fragile for a decade or more; thus DOD should initiate actions to lessen reliance on space while developing capabilities to reconstitute critical lost or degraded space assets within hours (Figure 11). Some of the options that could be considered entail non-space alternatives. For example, ISR sensors, communications, and other payloads could



be flown on “near-space” lighter-than-air unmanned aerial systems. Research and development work already has been conducted in this area. What is needed is a research approach leading to fielded operational platforms and systems.

Likewise, next-generation weapon systems such as the F-22 Raptor and the Joint Strike Fighter, as well as certain other/older platforms like the F/A-18 and F-15E, are being fielded with highly capable radar and other sensors. Networking these potential sources of “unconventional ISR” via common data-linked airborne and surface communication gateways could complement space-based capabilities in high demand. Another area worth investigating is launch-on-demand, operationally responsive space capabilities. These small, lower earth orbit satellites could provide an ability to rapidly reconstitute at least some capability in the wake of a catastrophic attack against space-based assets. Efforts to flight test and field such systems should continue.

Space Capability	Orbit	Vulnerability Kinetic/Non-kinetic	Alternate Sources	Reconstitution Priority	Reconstitution Need (within hours)
Imagery Intelligence	LEO	High/High	Aircraft and UASs	2	UAS, NT-ISR, LTA UAS
Satellite Communications	LEO & GEO	LEO High/High GEO Low/High	Terrestrial towers, line-of-sight and airborne relay	4	ORS, HAE UAS, LTA UAS
Precision Navigation	MEO	Medium/ Medium	No alternate source	1	Pseudolites, LTA UAS
Signals Intelligence	LEO & GEO	LEO High/High GEO Low/High	Aircraft and UASs	3	ORS, UAS, LTA UAS
Weather	LEO & GEO	LEO High/High GEO Low/High	Terrestrial observations and aircraft	5	ORS, LTA UAS

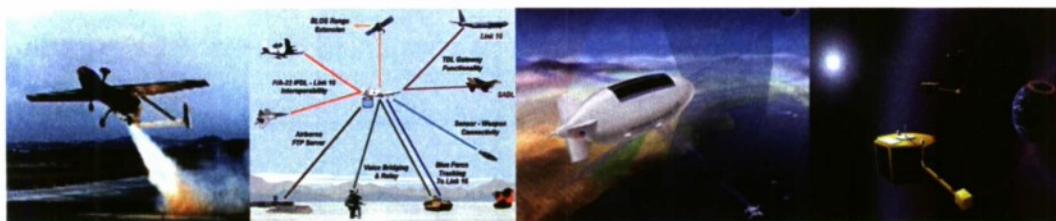


Figure 11. Reconstituting Degraded or Lost Space Capabilities



### RECOMMENDATION: OPERATING IN A DEGRADED SPACE ENVIRONMENT

The Assistant Secretary of Defense for Networks and Information Integration ASD (NII), (DISA), and the Services should field a GIG that has redundant communication means and waveforms with auto-communication rerouting capabilities.

Services field systems with highly accurate and reliable inertial measurement units and incorporate “atomic clocks on a chip” for timing signal.

Services ensure a mix of terminal guidance systems and weapons in the nation’s arsenal—not only GPS-guided weapons.

Joint Forces Command incorporate realistic exercise scenarios into joint and combined exercises that emphasize degraded space capabilities.

Services incorporate training in degraded space environment on live-fire training ranges.

---

### *Cyber Warfare Against Information and Networks*

Potential adversaries have growing capability to disrupt, compromise, and corrupt the information and networks that have become so critical to U.S. military operations. Not only are U.S. military forces vulnerable, but cyber attacks against civilian infrastructure also have significant coercive and destructive potential against the United States, its allies, and partners. Such attacks may offer adversaries a high-leverage option to coerce the United States or deter U.S. actions.

In some cases, adversary capabilities may exceed U.S. cyber capabilities, especially in terms of the workforce that can be brought to bear for cyber warfare. The relevant technology is global and accessible, which means that the United States is unlikely to have a significant advantage. Moreover, highly-skilled technical people are a critical component of the capability and some potential adversaries have a much larger base of such people than does the United States.

Highly visible Internet attacks tend to focus attention on remote access attacks. But close access penetration and life cycle insertion may be the most serious threats, because they are the hardest to defend against and can affect the most sensitive U.S. systems. The nation should expect that peer and near-peer adversaries will be well-practiced in close access and life cycle insertion, as well as remote access attacks. Yet this area is getting the least attention.

There are many ongoing efforts to improve the U.S. cyber warfare posture, but significant shortcomings remain. Findings from this study suggest that there is little operational understanding of the consequences of cyber attacks, as well as major information assurance deficiencies. There is a lack of “traditional” intelligence support for cyber defense. Cyber command and control concepts are at rudimentary stages and situational awareness is weak. Programmatic development and acquisition program test and evaluation shortfalls exist. Organizational authorities—policy and legislation—are at odds with borderless cyberspace. Further, the nation lacks a tenable deterrent capability.

Confronting the cyber threat requires not only an effective cyber defense, but also preparation of operational forces to function in the degraded environment caused by cyber attack. Contingency plans and processes must be carefully considered and practiced in advance.

#### **RECOMMENDATION: U.S. CYBER WARFARE POSTURE**

The Chairman, Joint Chiefs of Staff, combatant commanders, and service chiefs provide greater buy-in and participation by operations community in countering cyberspace threats. Principal emphasis should be on more rigorously addressing cyberspace threats in exercises and experiments to understand operational effectiveness in the face of such threats.

Under Secretary of Defense for Personnel and Readiness, in conjunction with ASD (NII)/DOD Chief Information officer (CIO) and the service chiefs, implement efforts to establish an adequate workforce for cyberspace defense to include personnel requirements and sources, establishing career fields, and ensuring enhanced training and leader development.

USD (AT&L), working with the Director, Operational Test and Evaluation and the ASD (NII)/DOD CIO, establish an information assurance test and evaluation process that spans the life cycle of systems.

The Secretary of Defense, with the Secretary of Homeland Security, determine how DOD can best contribute to national cyber defense planning and be prepared to assume greater responsibilities during major cyber attacks affecting U.S. government and civilian infrastructure.

---

### ***Cross-cutting Considerations***

In each of the cases described here, military forces must be able to operate effectively and successfully for extended periods of time in degraded environments. This is a tall order but critically important. Potential asymmetric capabilities will have catastrophic consequences in future combat operations unless the nation takes action now to offset current vulnerabilities. DOD must reconsider investments in countering WMD and prepare to conduct operations in space and cyberspace.

Warfighting against adversaries who employ these asymmetric capabilities will be a new experience for the United States. Thus, it is necessary to develop an intellectual foundation for the concepts of operations and rules of engagement that will serve to enhance training and leadership development, and bridge the gaps in asymmetric aspects of operational warfighting that currently exist. Both offensive and defensive operations must be integrated if U.S. forces are to be optimally effective. Enhanced experimentation, exercises, and assessments are all necessary to gain experience, measure progress, and refine operational concepts.

### **Strategic Communication: Another Instrument of U.S. Power**

---

Defending U.S. interests against future adversaries will require more than just military might. It may also call for the United States to rely on other instruments of U.S. power—such as diplomacy, economic and financial sanctions, and strategic communication. The instrument of strategic communication is vital to America's future, and must be transformed at strategic and operational levels. The United States and its partners face an array of transnational and state-based threats, as well as an abundance of opportunities. These threats and opportunities vary greatly in their nature and potential effect, but they present a common challenge. That is, they require a strategic communication instrument with sustained impact and far greater capacity to understand, engage, and influence global populations on issues of consequence.

Strategic communication is a dynamic process that integrates the development, implementation, assessment, and evolution of public actions and messages in support of America's interests at home and abroad. Too often, political and military leaders treat strategic communication only as crafting and disseminating messages, as something done by someone else, or as an afterthought in determining strategic priorities. But strategic communication today calls for a radically different approach—one that incorporates persuasive, cooperative, and coercive instruments

of national power. It is necessary before, during, and after armed conflict and is essential to formulating executive national strategies. Strategic communication is a proactive, sustained, and coherent set of activities in support of U.S. strategic objectives that includes:

- **Understanding** global attitudes and cultures
- **Advising** policymakers, diplomats, and military leaders on public opinion implication of policy choices
- **Engaging** in a dialogue of ideas between people and institutions through programs that support the national interest
- **Influencing** attitudes and behavior through communication strategies
- **Measuring** the impact of activities

Strategic communication is a central responsibility of the President and senior government leaders, and is conducted by a wide variety of civilian and military practitioners. Its successful use depends on shared knowledge and strong, adaptive networks both within government and between government and civil society.

Success in strategic communication depends on:

- deep comprehension of the identities, attitudes, cultures, interests, and motives of others
- awareness by leaders and practitioners that *what we do* matters more than *what we say*
- institutionalized connections between a wide variety of government and civil society partners in the United States and abroad
- a durable model of strategic direction that adapts quickly, transforms stovepipes, integrates knowledge and functions, and builds next generation skills and technologies

While “all politics is local,” all communication is now global. Gaps between what national leaders say and what the nation does and gaps between what national leaders say and what others hear have strategic consequences. These “say-do” and “say-hear” gaps affect U.S. interests in ways that can be measured in lives, dollars, and lost opportunities. In general, the nation continues to underestimate these impacts, to the disadvantage of the United States.



Successful strategic communication requires an interactive relationship between senders and receivers. People understand and relate to ideas and information when they identify with what is conveyed. Successful communicators enlist interest through credible symbols (actions, images, and words) and evoke common ground by focusing on culturally independent concepts that are valued globally—human dignity, health, personal safety, education, the environment, and economic well being—and thus form the basis for building support and mobilizing allies.

An important aspect of strategic communication is realizing that what we say and value is not always what others hear. Words such as “democracy,” “rule of law,” and “freedom” have different meanings in different cultures at different stages of their development. Understanding these differences is a crucial first step in successful strategic communication. Also crucial is an understanding that actions are more important than carefully crafted messages. Images, body language, and media context are messages too, and can conflict with actions and words.

### ***Strategic Communication Must Be Agile***

Events and actions provide the opportunity for interpreting long-lived themes in new, fresh, and particularly effective ways. Some events and actions—by the United States and by adversaries—can be anticipated. In those cases, messages can be thought out and prepared for use at an appropriate time. But other events and actions are surprises and require messages to be adapted in light of the situation. Thus, agility is critical.

Events and adversary actions present opportunities both to improve the effective communication of overall messages as well as to delegitimize actions and messages of our opponents (Figure 12). But 24 hour-a-day media operations make rapid response to events challenging. Delayed response allows the media to interpret the meaning of events, and each organization’s interpretation is affected by different cultural context. In the end, reports and messages can be conflicting and in competition.

Thus, offensive strategic communication can use opponent’s inconsistencies as opportunities to put forward a consistent and compelling story that can change beliefs of those looking at the situation from the outside. As a result, it is important to strengthen current efforts in offensive communication that exist in the Department of States (Counter Terrorism Communication Center), the

combatant commands (Rapid Response Units), and to enhance tools and training for interagency media engagement.



**De-legitimize our opponents' messages and actions**



**Emphasize positive events and activities**

**Figure 12. Strategic Communication Must Be Agile**

While surprise events and actions require agility in strategic communication, the media transformation that has been underway for the past two decades has changed the way people access and share information, further supporting the need for agility and speed. Information today is viral, not broadcast, driven principally by the rise of the Internet and the global spread of satellite television. Google, YouTube, Wikipedia, blogs, chat rooms, and other sources of information abound through the Internet, where users pull information that is of interest to them as individuals. In contrast, traditional media pushes information to the listener. But as satellite and cable television have opened an abundance of alternative channels to international audiences, audiences are becoming polarized into smaller, targeted interest groups. As a result, traditional media are losing their influence.

Today, information spreads from user to user with tremendous speed and terrorists have asymmetric advantage in the use of media. They have fast response and great flexibility, enabled by a decentralized leadership with local autonomy. Moreover, they are unconstrained by considerations of truth. Their concern with communication is exemplified by actions that seem to have been planned with media attention as the primary objective. News is, by nature, bad news—so bombs sell, good deeds do not.

Because of the rise of the Internet and satellite television, state censorship of content is becoming much less effective and will ultimately become impossible. It is quite difficult to control information access on the Internet. Even though

some countries limit Internet connectivity through proxy servers that filter content, many users know how to circumvent these filters and the information they access gets passed along in other ways.

With so many pathways allowing information to reach people, the emphasis today should be much less on the physical mechanism for delivery than it has been in the past. The focus should be on message, credibility, and presence. But today, America suffers an image problem around the globe. This includes attacks on America's policies as well as suspicions of the nation's intentions. Thus, the challenge is to craft messages that will travel through this complex and variegated landscape.

### *Despite Progress, Much Remains to be Done*

When the DSB investigated the topic of strategic communication in 2004, it found "tactical achievements" in strategic communication, notably in public affairs coordination, U.S. broadcasting to the Middle East, and the embedded media policy of DOD. The board concluded, however, that despite the promise of statements calling for significant change in the President's National Security Strategy (2002), "the U.S. had made little progress in building and transforming its strategic communication assets."

Nearly four years later the board's view is more positive at the departmental level. The State Department has had strong, consistent leadership for more than two years in the office of the Under Secretary for Public Diplomacy and Public Affairs. There is new leadership in the Broadcasting Board of Governors. The 2005 Quadrennial Defense Review included a Strategic Communication Working Group, which led to approval of a Strategic Communication Roadmap and creation of a Strategic Communication Integration Group by the Deputy Secretary of Defense. In May 2007, the interagency Strategic Communication Policy Coordinating Committee issued a "U.S. National Strategy for Strategic Communication and Public Diplomacy." These developments and a number of positive changes at the operational level are discussed in this report.

Nevertheless, the current study finds reasons for continued concern. Positive changes within organizations are real, but they depend to a considerable extent on the skills and imagination of current leaders. These changes must be evaluated, and those that work should be institutionalized. Resistance from traditional organizational cultures continues. Resources for strategic communication have increased, but they fall substantially short of national needs.



The primary concern is that fundamental transformation in strategic communication has not occurred at the strategic and interagency level. Reforms within organizations are important, but they are not a substitute for strong White House leadership and enduring, flexible networks that connect strategies and capabilities, departments and agencies, government and civil society.

### *Leverage National Capacity*

The challenges associated with strategic communication are increasing in complexity. As described, information technology and media interface have been transformed. Instead of top-down “one-to-many” in which limited media vehicles communicated with the masses, today’s environment is a bottom-up “one-to-many” in which one individual is able to reach many individuals with a sophisticated communication package at negligible expense.

The United States will fail in meeting 21<sup>st</sup> century national security challenges if it does not take existing government collaboration with civil society to a new level—leveraging national capacity. Challenges of the kind and magnitude the world now faces cannot be met by states alone. This will mean strengthening traditional partnerships with non-profit organizations in exchanges, broadcasting, and other government functions. Much more needs to be done to harness the knowledge, skills, creativity, and commitment of academic, non-profit, and business communities in more imaginative ways.

Thus, talent, resources, expertise, and creativity must be mobilized and utilized both within and outside of government. Resources such as Sesame Street Workshop, Community Radio, Peace Corps, and DOD Regional Centers can play a role. Stronger public-private partnerships should be encouraged along with engaging capabilities of new philanthropy and social entrepreneurship (such as the Gates Foundation). Marketing and entertainment talent can be brought to bear as well as relevant celebrities. “Individuals as nodes” are becoming networked communicators, making public engagement a strategic, diplomatic, and economic imperative.

For the U.S. government to accomplish this more challenging task will require a comprehensive discipline that includes situational awareness, sustained action, unity of messages, and resources commensurate with the task. Government departments alone cannot develop the deep understanding of cultures, influence networks, or information technologies that can be achieved through close collaboration with civil society. Their efforts will benefit from the expertise,



methods, core data, and best practices available outside government. In recommending the creation of an independent Center for Global Engagement, the intent is not to duplicate or draw funding from effective government strategic communication activities. Rather, the goal is to create an entity that is accountable, that operates in the public interest, that is outside but closely connected with government, and that will greatly enhance an instrument that can only succeed with shared knowledge and adaptive networks between government and civil society.

### *Sustained White House Leadership*

Strategic communication requires sustained senior leadership at the White House level that focuses exclusively on global communication and directs all relevant aspects of national capacity. These leaders must have authority as well as responsibility—authorities to establish priorities, assign operational responsibilities, transfer funds, and concur in senior personnel appointments. Importantly, these senior leaders must have direct access to the President on critical communication issues when policies are formulated and implemented.

After looking closely at this issue for nearly a decade, the DSB has reached the following conclusions. Presidents shape the nation's strategic communication in powerful ways. They require permanent structures within the White House that will strengthen their ability to understand and communicate with global audiences. Coordination committees may occasionally work well, but they are not a substitute for strategic direction that is durable and empowered. Leaders in departments have full-time management responsibilities that limit their ability to direct and coordinate at the interagency level. Departments and agencies have constraints that make it difficult for them to think and act in interagency terms. *Ad hoc* "czars" and incremental changes to national security structures designed generations ago are not the answer. There is no such thing as a "perfect" strategic direction model. Talented, competent leadership will determine success, but good leaders function best in good structures.

Election cycles and episodic commitment have shaped and limited strategic communication for decades. Today, America needs a new vision, new structures, and new legislated authorities. These can only be achieved with Presidential direction and the focused actions of leaders in Congress.

## *Recommendations*

### **RECOMMENDATION: THE CENTER FOR GLOBAL ENGAGEMENT**

**The President, congressional leaders, and interested organizations outside government collaborate to create an independent, non-profit, and non-partisan Center for Global Engagement (CGE).**

Three principles should guide the establishment and work of the Center for Global Engagement. First, that the direction, planning, and execution of the government's strategic communication instrument are government responsibilities. Second, that government cannot succeed in carrying out its responsibilities without sustained, innovative, and high-quality support from civil society. Third, that the academic, research, business, and non-profit communities offer deep reservoirs of untapped knowledge, skills, credibility, and agility needed to strengthen strategic communication.

The Center for Global Engagement should be a:

- 501(c)(3) corporation with an independent director and board of directors
- means to motivate and attract civil society's best and brightest
- hub for innovation in cultural understanding, technology, and media
- repository of expertise
- magnet for innovative ideas
- means to institutionalize continuity and long-term memory
- focus for experimentation and project development

The study recommends that Congress provide the Department of State with \$500,000 to develop a charter that will define the mission, structure, and operations of the CGE. The Department should award these funds through a competitive grant to an organization or group of organizations that will prepare and execute a business plan leading to the creation of the CGE as an independent corporate entity (one option could be to extend the mission of an existing federally funded research and development center or 501(c)3 corporation).

Thereafter, Congress should provide sustained funding for the CGE through a line item in the Department of State's budget. This should be new money appropriated to the Department. Congress should provide the CGE with an

initial appropriation of \$50 million in fiscal year 2009. The objective should be steady funding growth, consistent with performance and use by multiple government agencies, to \$250 million during the first five years.

The CGE should:

- respond to multi-agency government taskings, coordinated through a National Security Council Deputies Committee for Strategic Communication
- provide deep understanding of cultures and cultural dynamics, core values of other societies, and media and technology trends
- provide core data, best practices, and an opinion research clearing house in support of government-sponsored strategic communication programs
- assess the effectiveness of national strategic communication activities and programs
- collaborate with independent organizations that promote universal values, cultural understanding, and global engagement
- maintain a repository of strategic communication talent, skills, and capabilities
- attract fellows from the academic, non-profit, and business communities, and from government

#### **RECOMMENDATION: LEADERSHIP**

**Create a permanent strategic communication structure within the White House.**

This structure should have the following elements:

- Deputy National Security Advisor and Assistant to the President for Strategic Communication
- Deputies Committee for Strategic Communication
- Strategic Communication Policy Committee, chaired by the Deputy National Security Advisor and Assistant to the President for Strategic Communication, to include all departments and agencies with substantial strategic communication responsibilities

- Associate Director for Strategic Communication in the Office of Management and Budget
- legal and regulatory authorities as necessary for the Deputy National Security Advisor and Assistant to the President for Strategic Communication to:
  - (1) assign operational responsibilities, transfer funds, and concur in personnel appointments
  - (2) provide guidance on strategic communication to an independent Center for Global Engagement

#### **RECOMMENDATION: SCIENCE AND TECHNOLOGY OPPORTUNITIES**

**The Department of Defense should make greater use of existing tools and technologies to support strategic communication.**

For example, existing science and technology capacity can be used to:

- identify nodes of influence through network analysis
- support communication and media analysis with machine translation
- understand viral information flows and influences
- utilize innovative evaluation and measurement methodologies (*e.g.*, sentiment detection/analysis).

The study recommends that \$50 million a year be invested to advance knowledge in these areas and that this research budget be managed by DARPA, the National Science Foundation, and the intelligence community. The task force recognizes the current but disparate efforts in these areas and recommends vigorous engagement across the strategic communication community to share the existing knowledge base.

#### **RECOMMENDATION: DEPARTMENT OF STATE**

**The Under Secretary of State for Public Diplomacy and Public Affairs should be given enhanced policy, budget, and personnel authorities.**



The study recommends a significant increase in the budget for the State Department's public diplomacy programs, including exchanges over a five-year period. The budget should be tripled and additional funds used in the following areas:

- exchanges (*e.g.*, Fulbright, international visitor leadership program, international military education and training)
- Americans studying/conducting research abroad
- recruitment, training, and deployment of additional public diplomacy positions
- support for strategic communication and public diplomacy activities of the U.S. military's combatant commands
- Internet, websites, blogging, Rapid Response Units, and Digital Outreach Teams
- opinion, attitude, and behavioral research and evaluation of/for public diplomacy programs
- book translation programs
- utilization of sports and entertainment figures as cultural diplomats
- training and partnerships with key civil society activists (journalists, local media, civic organizations)
- online English language (English as a second language) programs focused on marginalized young Muslim populations
- public-private partnerships targeted at economic development and job creation in key strategic nations (Lebanon, Pakistan, Iraq)

In addition, the study recommends that a senior State Department public diplomacy representative be assigned to each combatant command.

#### **RECOMMENDATION: BROADCASTING BOARD OF GOVERNORS**

Conduct a review of the mission, structure, funding, and performance of the Broadcasting Board of Governors, as an integral element of the overall U.S. strategic communication capability.

---

The following should be part of the review:

- current media mix
- relationship among the U.S. international broadcasting services (such as Voice of America, Radio Free Europe/Radio Liberty, Radio Free Asia)
- utilization of new communication media
- new models for utilization and funding of news and program services
- language priorities (currently 60 languages)
- audience research (*e.g.*, market research, media usage, impact)
- management structures and relationships with the executive branch

The DSB is pleased with the passage of Section 316 of the 9/11 bill that provides the President new authority to support requirements for surge broadcasting. The administration and Congress are urged to implement procedures and funding measures to utilize this much-needed authority when a surge requirement is identified.

#### **RECOMMENDATION: DEPARTMENT OF DEFENSE**

**Create a permanent Deputy Under Secretary of Defense for Strategic Communication, reporting to the Under Secretary of Defense for Policy.**

**Significantly increase the strategic communication budgets of each combatant commander.**

---

This new office of the Deputy Under Secretary of Defense for Strategic Communication would include senior representatives from the Office of the Secretary of Defense for Public Affairs, the Joint Staff, and the Under Secretary of Defense for Intelligence. The office would review and coordinate all information activities aimed at foreign governments across public affairs and information operation domains.

Strategic communication funding for each combatant commander should be tripled above current levels and identified within a separate budget for each geographic combatant command. Additional funds should be used for the following activities:

- task federally funded research and development centers (FFRDCs), such as the Institute for Defense Analyses and RAND, to conduct cultural

analysis and program development in each combatant commander's area of responsibility

- provide communications infrastructure in support of stability operations and disaster relief operations
- increase public affairs presence at each combatant commander to support security cooperation
- increase collaborative planning and experimentation with nongovernment organizations

**Increase engagement in support of strategic communication.** For example:

- increase hospital ship and crew activation to support security cooperation programs
- utilize Corps of Engineers capabilities to support programs for disaster relief, flood control, and infrastructure development (security cooperation)
- release reconnaissance products for environmental studies, crop management, weather forecasting, food and water supply management, deforestation, and other similar activities
- create opportunities for civil sector participation (*e.g.*, media, nongovernment organizations, academics) at the National Defense University, the military service colleges, and Centers for Regional Security Studies

Finally, the study recommends that psychological operations be relabeled according to whether they are in support of military operations or other activities, such as security cooperation and DOD support to public diplomacy.

#### **RECOMMENDATION: ACTIONS FOR TODAY**

Many of the specific actions identified previously can be implemented immediately and are identified here.

The DSB recommends that the Department of Defense and Department of State implement immediate actions as follows:

- Establish and enhance combatant commander's budgets for strategic communication to:

- fund FFRDCs (such as the Institute for Defense Analyses, RAND) to conduct cultural analysis and program developments in the area of responsibility
- provide communications infrastructure in support of stability operations and disaster relief operations
- Increase Defense Department support for strategic communication by, for example:
  - increasing hospital ship and crew activation to support security cooperation programs
  - releasing reconnaissance products for environmental studies, crop management, weather forecasting, food and water supply management, deforestation
  - creating opportunities for civil sector participation (*e.g.*, media, nongovernment organizations, academics) at the National Defense University, the military service colleges, and Centers for Regional Security Studies
- Expand the Department of State's strategic communication funding and for such activities as:
  - online English language programs focused on marginalized young Muslim populations
  - Internet, websites, blogging, Rapid Response Units, and Digital Outreach Teams
  - public-private partnerships targeted at economic development and job creation in key strategic regions (*e.g.* Lebanon, Pakistan, Iraq)

## Final Thoughts ---

In the future, more nations and some non-state actors will be able to challenge U.S. interests. Technology proliferation, which provides access to an increasingly wide range of weapons, tools, and skills, on balance, favors U.S. adversaries whose adaptable characteristics enable them to more quickly take advantage of this evolving environment. Further, the U.S. homeland is not easily secured and, therefore, is a potential area of attack, with considerable consequences. Attacks on critical military infrastructure in the homeland will impede deployment and supply. Attacks on civilians will split U.S. forces between fighting abroad and responding to catastrophes at home. Taken



together, the cost to deter or defeat future adversaries is rising—costs defined along many dimensions to include military lives, civilian lives, money, civil liberties, daily comfort, economic health, and global reputation.

Although costs are rising, the United States is not making material progress in reducing the costs. Intelligence is inadequate to motivate and prioritize investments. No adversary can exercise all options, but the nation has little insight into what capabilities or options can be exercised or are likely to be. Furthermore, lack of action on the part of adversaries has become an excuse not to prepare—as it is true that, by and large, unconventional weapons and operational concepts have not been used by adversaries (with cyber attacks being the exception). In addition, DOD's combat capabilities abroad depend on other federal, state, and local capabilities at home, so reducing costs will have to be done in partnership with many others. But perhaps most important, is the fact that the nation does not conduct realistic exercises of the sort that would illuminate the degree to which military capabilities will be degraded. As long as the nation chooses inaction, circumstances will continue to worsen.

Despite the challenges described herein, however, circumstances can be materially improved. The U.S. can achieve its national objectives by taking a combination of actions that will have an impact on costs. The first set of needed actions are to reduce the “cost” to the United States of the non-traditional weapons and non-traditional operational concepts that future adversaries are likely to use. As described in this summary, and in further detail in the main report, key actions include:

- Institute a vastly better exercise regime with unfettered red teams. Challenges to U.S. forces should include fighting through a limited nuclear attack or other WMD attack; fighting with degraded information infrastructure and disrupted space assets; responding to attacks on civilians in the homeland with the aid of local, state, and federal organizations; and maintaining deployment and supply even with attacks on critical defense infrastructure in the homeland.
- Reduce the likelihood that the information system will be a target.
- Prepare for war in space.
- Manage the malignancy of nuclear proliferation.
- Improve foreign intelligence, addressing the most critical intelligence gaps.

- Improve domestic intelligence to protect “the exposed rear.” The New York Police Department’s successful domestic intelligence efforts can serve as a model.
- Prepare to work with local, state, and federal domestic organizations in event of an attack on the homeland.
- Take the dominant radiological threat “off the table”

The second set of actions involves shaping U.S. will and the will of adversaries and neutral parties to pay the costs. This will involve strengthening other instruments of foreign policy, in particular strategic communication.

If not prepared for the worst, and not backed by strong political will, the Department of Defense could find itself on the losing side of the next stressing war. Thus, DOD must begin to take immediate action, even as it fights the current war, to make sure it is ready for the next—a war that could well be even more stressing than the war the nation fights today. If America is ready, there is a good chance that the next war will not have to be fought, as readiness will serve to deter our adversaries from acting. If the nation is not ready, the probability of fighting the next war is high and the outcome likely to be uncertain.

## Terms of Reference



ACQUISITION,  
TECHNOLOGY  
AND LOGISTICS

## THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3010

FEB 02 2007

### MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference -- Defense Science Board 2007 Summer Study on  
Challenges to Military Operations in Support of National Interests

The United States capability in conventional warfare is unmatched by any other state for now and the immediate future. The success in Operation DESERT STORM followed by even greater success a decade later in the initial phases of Operations ENDURING FREEDOM and IRAQI FREEDOM demonstrate an overwhelming ability to continually grow conventional capability and outmatch opponents.

However, the same overmatch does not exist across the conflict spectrum and is unlikely to exist in the conventional space forever. For example, the Soviet Union threatened the existence of the United States along nuclear and ideological lines and seriously threatened U.S. interests with conventional arms. Russia retained sufficient nuclear capability to threaten U.S. existence, but that threat is no longer coupled with the same ideological and conventional threat. The growing proliferation of nuclear weapons may challenge U.S. conventional forces in some regions or thwart U.S. interests. Finally, we have to expect WMD proliferation, e.g., biological, in general. Will WMD proliferation transform unexpected adversaries into challengers sufficiently capable to threaten the existence of the U.S. or at least thwart U.S. interests?

Asia's economic growth may enable several states to compete along conventional lines if they so choose. An important part of Asia's growth is driven by globalization of technology and manufacturing prowess that discounts historical DoD advantages in these areas. The worst-case scenario results in a technologically inferior U.S. vis a vis an opponent. There are also indications that opponents may not choose to confront the U.S. head to head with conventional forces: asymmetric warfare is the province of states as well as of terrorists and insurgents, e.g., the recent conflict in Lebanon demonstrated gaps in conventional vs. asymmetric forces. Finally, the U.S. may choose capabilities and resultant force structures that provide opponents unrecognized vulnerabilities for their exploitation. Although these types of challenges may not threaten the existence of the United States, they may prove sufficiently challenging to justify serious consideration and planning to mitigate the effect on U.S. interests.



In addition, the U.S. Armed Forces will likely face: continuing and long lasting stabilization and reconstruction operations; an increasing number of humanitarian missions driven by epidemics and AIDS, climate change, famine and water shortages, religious and tribal strife; and more instances of domestic catastrophe support, like Katrina. These responsibilities will inevitably detract from capabilities for deterring and defeating competitors who could challenge military operations.

Further, nowadays competition is intrinsically global. On one hand, we need the capability for very swift deployment anywhere on Earth to counteract "blitzkrieg" tactics, capability for decisive deployment of massive force to counteract a peer, and capability for sustained deployment for operations that might take years. On the other hand, attacks on our homeland must be not only anticipated but expected; and the very same resources needed for foreign expeditions, e.g., the Reserve, might be needed for protection at home.

As the world evolves in the 21<sup>st</sup> century, the Department of Defense must anticipate future stressing wars. What would a challenger look like and how would it successfully challenge military operations? Will states attempt to achieve peer status in a conventional force-on-force conflict, or will some other strategy prove successful? If not, what will they attempt to enable them to maintain their interests? Under what circumstances might a coalition or transnational group successfully challenge military operations? What are the metrics for success in this environment? Are there innovative technologies, systems or operational concepts that can be applied to this subject before it becomes a national crisis?

Specifically the Summer Study should:

- (1) Review previous and ongoing studies regarding stressing wars;
- (2) Identify defining parameters for challenges to military operations (e.g., physical size, population, technological prowess, and denial and deception);
- (3) Assess capability gaps;
- (4) Identify possible solutions. At a minimum, the Summer Study should assess technological, operational, and policy oriented solutions.

The study will be co-sponsored by the Under Secretary of Defense for Acquisition and Technology and the Under Secretary of Defense for Policy. Dr. Craig Fields and Mr. Rich Haver will serve as Chairmen of the Task Force. Mr. Todd Lowrey, OUSD(P) will

serve as Executive Secretary; and Commander Cliff Phillips, USN, will serve as the DSB Secretariat Representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of title 18, U.S. Code, section 208, nor will it cause any member to be placed in the position of acting as a procurement official.



Kenneth J. Krieg

## Study Participants

### CHAIRMEN

Name	Affiliation
Dr. Craig Fields	Private Consultant
Mr. Richard Haver	Northrop Grumman Corporation

### EXECUTIVE SECRETARY

Todd Lowery	OSD(P)/SOLICIC
-------------	----------------

### FUTURE OF WAR PANEL

<b>Chairs</b>	
GEN Bill Hartzog	Burdeshaw
Dr. Joe Markowitz	Private Consultant
<b>Members</b>	
Paul Davis	RAND
Bert Fowler	CA Fowler Associates
Dr. Ted Gold	Private Consultant
MG Kenneth Israel USAF (Ret.)	Lockheed Martin Aero
Bob Mikelskas	MITRE
Bill Murray	Alphom, LLC
MG Rich O'Lear	Lockheed Martin
Dr. Joe Rosen	Dartmouth-Hitchcock Medical Center
MG Robert Scales	Private Consultant
Dr. James Wade	Defense Group
Mike Wheeler	DTRA
<b>Government Advisors</b>	
LTC Kirklin Bateman	Army G-35, DAMO-SSP
COL Jeff Bearor	USMC
Peter Bechtel	HQDA DCS G-3/5/7
Thomas Behling	OSD/OUSSI
Maj Trudy Caldwell	Bechtel's Staff (HQDA DCS G-3/5/7)
Dr. James Forest	West Point (USMA)

Dr. Ellen Klein	OSD/GSA--Detainee Affairs
COL Daniel Klippstein	HQDA DCS G-3/5/7
MAJ John Livingstone	HQDA, G-3/5/7
Col Louis Michael USA (Ret.)	Defense Group Inc
Dr. Mac Owens	Naval War College (1D)
Charles Swett	OSD Policy
Robert Vickers	ODNI

**TECHNOLOGY ASSESSMENT PANEL**

<b>Chairs</b>	
Larry Lynn	Private Consultant
Bob Stein	Private Consultant
<b>Members</b>	
Dr. Larry Brandt	Sandia National Laboratories
Dr. Regina Dugan	RedXDefense
Dr. Kevin Fall	Intel Corporation
Dr. Milton Finger	Lawrence Livermore National Laboratory
Mr. Jim Gosler	Sandia National Laboratories
Dr. Bernadette Johnson	MIT Lincoln Laboratory
Dr. Duane Lindner	Sandia National Laboratories
Mr. Walter Morrow	MIT Lincoln Laboratory
Mr. Jim Shields	Draper Laboratory
Dr. Wayne Shotts	Lawrence Livermore National Laboratory
Dr. Ann Marie Skalka	Fox Chase Cancer Center
Dr. James Tour	Rice University
Dr. Rich Wagner	Los Alamos National Laboratory
Dr. Bruce Wald	Private Consultant
Mr. Larry Wright	BAH
Dr. Gerry Yonas	Sandia National Laboratories
<b>Government Advisors</b>	
Dr. Jon Calomiris	United States Army Nuclear and Chemical Agency
Mr. Christina Filarowski-Sheaks	Office of the Secretary of Defense



Dr. Stephen Morse	National Center for Preparedness, Detection, and Control of Infectious Diseases Coordinating Center, Centers for Disease Control
Ms. Cecilia Phan	The Joint Staff, Directorate for Command, Control, Communications, and Computer Systems
Dr. Lisa Rotz	National Center for Preparedness, Detection, and Control of Infectious Diseases Coordinating Center, Centers for Disease Control
David Thomen	Army G-3/5/7

#### NUCLEAR PROLIFERATION PANEL

<b>Chair</b>	
Dr. Brad Roberts	Institute for Defense Analyses
<b>Members</b>	
Dr. Dan Chiu	Institute for Defense Analyses Joint Advanced Warfighting Program
Dr. Lewis Dunn	SAIC
John Hinton	Sandia National Laboratory
Douglas Lawson	OATSD(NCB/NM)
Dr. James Miller	Center For a New American Security
Jim Thomas	Applied Minds, Inc.
Dr. Victor Utgoff	Institute for Defense Analyses
Major Stephanie Vaughn	US Army Nuclear and Combating WMD Agency
<b>Government Advisors</b>	
Larry Brant	Sandia National Laboratories
Melanie Elder	ODNI/National Counterproliferation Center
Ms. Rebecca Hersman	National Defense University
Col Chuck Lutes USAF	National Defense University
Mike Wheeler	DTRA

**DEFENDING AGAINST DOMESTIC CATASTROPHE IN WAR TIME PANEL**

<b>Chairs</b>	
Dr. Bill Howard	Private Consultant
Mr. Robert Nesbit	MITRE
<b>Members</b>	
Mr. Jerry Buckwalter	Northrop Grumman
Mr. Evan Wolff	Hunton & Williams LLP
<b>Government Advisors</b>	
COL Joseph Bassani	U.S. Northern Command
Mr. Jim Caverly	Director, Partnership & Outreach Division
Mr. John Humpton	HQDA ODCS G-3/5/7

**ENSURING DEPLOYMENT AND SUPPLY PANEL**

<b>Chairs</b>	
Dr. Miriam John	Private Consultant
Dr. Ronald Kerber	Private Consultant
<b>Members</b>	
Dr. John Cummings	Sandia National Laboratories
Maj Gen John Fenimore V, USAF (Ret)	J.H. Fenimore & Assoc, LLC
LtGen Rick Kelly USMC (Ret.)	LMI
Dr. Duane Lindner	Sandia National Laboratories
VADM Keith Lippert, USN (Ret.)	Accenture National Security Service, LLC
Ms. Nancy Suski	Lawrence Livermore National Laboratory
LTG David Teal USAF (Ret.)	Accenture National Security Services
Ms. Nancy Wilson	Association of American RR
<b>Government Advisors</b>	
COL Joe Bassani, USA	NORTHCOM
Mr. Bill Bryan	OSD(P)/ASD/HD
Mr. James Caverly	DHS
Mr. G. Gurvais Grigg	FBI
Mr. Lacey Hughes	HQDA DCS G-4
Mr. John Humpton	Department of the Army, G3

**WHAT WE KNOW AND DON'T KNOW: INTELLIGENCE PANEL**

<b>Chair</b>	
ADM Bill Studeman	Private Consultant
<b>Members</b>	
Joan Dempsey	Booz Allen Hamilton
Marty Faga	MITRE
Carol Haave	
Jeffrey Harris	LMCO
Jake Jacoby VADM, USN, (Ret.)	CACI, Inc.
Peter Marino	Private Consultant
Joseph Mazzafro	EMC2
Dave McMunn	McMunn Associates, Inc.
Barbara McNamara	CACI International
Rocky Rocanova	Rock & Nova
Earl Sheck	NGC
Dick Szafranski	Toffler Associates
Jim Woolsey	BAH
Mike Wheeler	DTRA
<b>Government Advisors</b>	
RC Porter	OSD
Michelle Van Cleave	National Defense University

**FIGHTING THROUGH ASYMMETRIC COUNTERFORCE PANEL**

<b>Chair</b>	
GEN Jim McCarthy, USAF (Ret.)	U.S. Air Force Academy
<b>Members</b>	
Russ Barber	Raytheon
LT GEN David Deptula	AF/A2
VADM Dave Frost USN (Ret.)	Frost & Associates, Inc.
Greg Gardner	Oracle Corporation
Dr. Ted Gold	Private Consultant
GEN Richard Hearney USMC (Ret.)	Private Consultant
Dr. Bob Hermann	Private Consultant

Richard Ivanetich	Institute for Defense Analyses
ADM Greg Johnson USN (Ret.)	
Jim Kurtz	Institute for Defense Analyses
Jim Kuzmick	Private Consultant
Zachary Lemnios	MIT Lincoln Lab
Maj. Gen Tim Lowenberg	Washington Army and Air National Guard
Dr. Jerry McGinn	Northrop Grumman Corporation
Dawn Meyerriecks	Private Consultant
RADM Norm Saunders USCG (Ret.)	SAIC
GEN Eric Shinseki	USA
<b>Government Advisors</b>	
Col Ronald Banks	USAF A9L
LTC Alan Eckersley	Army G-3/5/7
BG David Fadok	HAF
Darrin Gilchrist	
COL Clay Hicks	HQDA, G-33, Army Asymmetric Warfare Office, DAMO-ODA-P
BGen Jan-Marc Jouas	AF ISR Agency/CV
COL Doug King	USMC
CAPT Forbes MacVane	USN JFCC-NW J9
Ed Martin	Contractor, The Wexford Group International G3/5/7
Tim Moore	US Army Nuclear and Chemical Agency
John Plant	Contractor, The Wexford Group G3/5/7
LTC Dirk Plante	ARMY
Douglas Richardson	USSOCOM
Jeffrey Sawyer	DTRA
LTC Richard Voegtly	G3/5/7



## STRATEGIC COMMUNICATION PANEL

<b>Chair</b>	
Mr. Vincent Vitto	Private Consultant
<b>Members</b>	
Mr. Robert Coonrod	Private Consultant
Dr. Barry Fulton	Private Consultant
Prof. Bruce Gregory	George Washington University
Prof. Anita Jones*	University of Virginia
Dr. Robert Lucky*	Private Consultant
Dr. Mark Maybury	The MITRE Corporation
Ms. Leigh Warner	Private Consultant
<b>Government Advisors</b>	
Amb. Brian Carlson	State Department and OSD Policy
BG Mari Eder	Deputy Chief of Public Affairs, US Army
Mr. Morris Jacobs	U.S. State Department
Mr. John Matheny	OSD Policy
Mr. John Mills	OASD NII / CIO
RDML Frank Thorp	Joint Communications and SCIG, OSD

## ADDITIONAL GOVERNMENT ADVISORS

Maj Russell Buttram	USMC
COL Igor Gardner USAF	ISR Plans and Resources DCS, Intelligence
COL Brian Groft	DDUSA Nuclear and Combating WMD Agency
Dave Helvey	OSD Policy
Frank Hoffman	Marine Corps Warfighting Lab
COL Jonathan Jaffin	U.S. Army Medical Research and Material Command
CAPT Andrew King	Chief of Naval Operations (N81)
Dr. George Ludwig	U.S. Army Medical Research and Material Command
Terry Pudas	OUSDP
LTC Bryan Sparling	US Southern Command
Shawn Spencer	STRATCOM G-8

COL Jeffrey Springman	JCS J5
Captain Gene Wynne	USMC

**DSB REPRESENTATIVES**

Brian Hughes	DSB Office Executive Director
Andrew Chappell	DSB Office, USA
Maj Charles Lominac	DSB Office, USAF
Clifton Phillips	DSB Office, USN

**STAFF**

Barbara Bicksler	Strategic Analysis, Inc.
Sarah Canna	Strategic Analysis, Inc.
Julie Evans	Strategic Analysis, Inc.
Kelly Frere	Strategic Analysis, Inc.
Jennifer Howell	Strategic Analysis, Inc.
Anthony Johnson	Strategic Analysis, Inc.
Brian Keller	Private Consultant
Carla King	Strategic Analysis, Inc.
Philippe Loustaunau	Vista Consulting LLC
Toni Marechaux	Strategic Analysis, Inc.
Adam Savery	Strategic Analysis, Inc.
Ted Stump	Strategic Analysis, Inc.

## Presentations to the Study

Name	Topic
------	-------

### Plenary Sessions

#### JANUARY 24, 2007

Ms. Judy Kim	DOD General Counsel Briefing
Mr. John J. Hamre Center for Strategic and International Studies	Discussion
Dr. Stephen A. Cambone Former Under Secretary of Defense for Intelligence	Discussion
Mr. Ryan Henry Principal Deputy Under Secretary of Defense for Policy	Discussion

#### FEBRUARY 21, 2007

Aaron Friedberg Princeton University Dan Blumenthal, AEI Roy Kamphausen National Bureau of Asian Research	China
Mr. Richard Lawless Deputy Under Secretary of Defense for Asia and Pacific Affairs	Discussion
COL Joseph A. Bassani, USA U.S. Northern Command	Preparing for Domestic Catastrophes: Plans and Exercises
General James E. Cartwright Commander, U.S. Strategic Command	Discussion

**MARCH 21, 2007**

Mike Vickers Director, Strategic Studies, CSBA	Strategic Competition and Conflict with Near-Peer Competitors
Dr. Richard Danzig	Biowarfare
MG John Landry	Discussion
RADM Kenneth Deutsch Director, Warfare Integration (N6F)	Discussion

**APRIL 25, 2007**

Mr. William Neugent MITRE	Countering Sophisticated Cyber Threats
Mr. Peter Bechtel Director for the US Army Nuclear and Combating WMD Agency	Discussion
COL Jonathan Jaffin Acting Commander, U.S. Army Medical Research and Materiel Command	Future Army Medical Challenges

**JUNE 20, 2007**

Lt. Gen. David A. Deptula Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance	Discussion
--	------------

**Future of War Panel****MARCH 20, 2007**

Jim Thomas, Applied Minds, Inc.	Discussion on QDR (Secret)
Patrick Garrett, Bill Miles, & Joel Sepulveda, CIA	Chinese ASAT Launch (TS/SCI)
Charles Swett, OSD	QDR Scenarios
Joseph Rosen, Dartmouth-Hitchcock Medical Center and War Panel Member	Theory and Practice of War: Adversaries, Weapons, and Recommendations



**APRIL 24, 2007**

Maj Gen Rich O'Lear, Lockheed Martin & War Panel Member	Red Team Perspectives and Tasks (FOUO)
Jason M.K. Lyall Assistant Professor of Politics & International Affairs, Princeton University  LTC Isaiah Wilson, West Point	"Rage Against the Machines: Mechanization and the Determinants of Victory in Counterinsurgency Warfare"
Andy Marshall, Director, Office of Net Assessment, OSD	Past War Gaming (Secret)
Mackubin Thomas Owens Associate Dean of Academics and Professor of National Security Affairs, US Naval War College	The Logic of Future Force Planning

**MAY 22, 2007**

Dan Flynn, Office of the Director of National Intelligence	NIC Assessment (Secret/NOFORN)
---	--------------------------------

**JULY 17, 2007**

Robert O. Work Vice President, Strategic Studies, CBSA	Thinking About Future Warfare
Roy Evans Director of National Security Analysis Group, MITRE Corporation	Future of War (Secret)

**Technology Assessment Panel****FEBRUARY 20, 2007**

Norman Kahn, Program Manager Intelligence Technology Innovation Center	Biological Defense Research in the Intelligence Community
---	---

**APRIL 6, 2007**

Roundtable Discussion Kirtland, Air Force Base	Directed Energy Weapons
---	-------------------------

**APRIL 24, 2007**

Len Connell Sandia National Laboratories	Radiological Weapons Update
---	-----------------------------

Dr. Jason Lyall, Princeton University LTC Isaiah Wilson, West Point	Analysis of Asymmetrical Conflicts
Lawrence Gershwin, National Intelligence Council	Cyber threat technologies and Biotechnology Issues

**MAY 24, 2007**

Michael R. Rooney, Defense Threat Reduction Agency	Understanding High-Altitude Electromagnetic Pulse (HEMP) Effects and Uncertainties
--	--

**JUNE 21, 2007**

Brett Giroir, Director, Defense Sciences Office, Defense Advanced Research Projects Agency	Progress on Relevant Research at DARPA
--	--

**JULY 17, 2007**

John Vitko Jr, Chemical and Biological Division, Department of Homeland Security	An Overview of DHS/S&T Chem and Bio Programs
John MacKinney, National Homeland Security Research Center, US Environmental Protection Agency	RDD Threat and Technology Needs

**Nuclear Proliferation Panel****MARCH 22, 2007**

Dr. Melanie Elder (chair) National Counterproliferation Center  Mr. Vann H. Van Diepen, National Intelligence Officer for WMD and Proliferation  Ms. Marybeth Davis, Deputy Director for Strategy and Evaluation, National Counterproliferation Center  Mr. Joseph Pritchard, Deputy Director for Interdiction and Networks, National Counterproliferation Center	Proliferation Pathway Analysis
Ms. Rebecca Hersman, National Defense University	Future Nuclear Landscape: 2006-2011
Hon. Mr. Ryan Henry, Principal Deputy Under Secretary of Defense for Policy	Life in a Highly Proliferated World

**APRIL 17-18, 2007**

Dr. Vic Ugtoff, Institute for Defense Analysis	Extended Deterrence
---	---------------------

**MAY 22, 2007**

Chuck Lutes, National Defense University	Pathways and Alternative Futures
Jim Thomas, Applied Minds, Inc.	From Scenarios to Requirements
Daniel Chiu, Institute for Defense Analysis	Implications for the Nuclear Deterrent

**JUNE 19-20, 2007**

Mr. Greg Hulcher Office of the Secretary of Defense (Acquisition, Technology & Logistics)	"New Triad Implementation" (SECRET)
Mr. Tom Scheber National Institute of Public Policy	

**JULY 10, 2007**

Mr. Greg Hulcher Office of the Secretary of Defense (Acquisition, Technology & Logistics)	The New Triad Program of Record (SECRET)
Mr. Dennis Even Office of the Secretary of Defense – Program Analysis & Evaluation	
COL Pat Sharon Joint Staff (J-8)	Combating WMD Program of Record (SECRET)
Dr. John Hinton Sandia National Laboratories	Defining the Needed Nuclear Posture
Dr. Jim Miller Center for a New American Security	

**JULY 17, 2007**

Ms. Rebecca Hersman, National Defense University	Means to Inhibit Future Cascades
---	----------------------------------

## Ensuring Deployment and Supply Defending Against Domestic Catastrophe in War Time Joint Panel Meetings

### FEBRUARY 9, 2007

Mr. Don Latham	2003 DSB SS on DoD Roles & Missions in Homeland Security
Mr. Bob Stephan, DHS, Assistant Secretary for Infrastructure Protection	DHS Critical Infrastructure Approach
Dr. Miriam John/Dr. Ronald Kerber	Report of the DSB Task Force on Critical Homeland Infrastructure Protection

### MARCH 20, 2007

Mr. William Bryan, DCIP OASD (HD&ASA)	Update on DOD Defense Critical Infrastructure Program
Mr. Bob Nesbit, MITRE	DSB 2005 Summer Study on WMD
Maj Gen Tim Lowenberg, TAG for the State of Washington	National Guard Discussion
Ms. Nancy Wilson, American Association of Railroads	Partnership for Critical Infrastructure Security
GEN ( R ) Reimer, DFI International	Katrina Lessons Learned

### APRIL 24, 2007

Mr. Merrick Krause, DHS	National Infrastructure Simulation and Analysis Center and Critical Infrastructure Protection-Decision Support System
Maj Gen Fenimore, Private Consultant and Dr. Nancy Suski, Sandia National Laboratory	Citizen Preparedness
COL Joseph Bassani, USA, USNORTHCOM	NORTHCOM
Mr. Jim Kish, DHS	National Exercise Program
AD Dr. Vahid Majidi, FBI	FBI WMD Program

### MAY 24, 2007

Gen (R) Mike Carns, USAF, Private Consultant	DSB Energy Strategy Task Force
MG (R) Barry Bates, NDIA	Panel of Corporate Security Execs from Defense Industrial Base
Ms. Alane Andreozzi, DTRA	A Kele Exercise
Mr. Carl Brown, DTRA	BioNet
Colonel Joseph Bassani, USNORTHCOM	NORTHCOM



## JUNE 11, 2007

LTG C. V. Christianson, J-4 COL Ed Hatch, JFCOM Mr. Alan Banghart, DLA	OCONUS Deployment & Sustainment Panel
Mr. Ronald Krisak, IDA	Noble Resolve
Healthcare: Mr. Chris Lake, BLU-MED Response Energy: Mr. Stan Johnson, Manager Situation Awareness & Infrastructure Security, North American Electric Reliability Corporation IT: Mr. Guy Copeland, CSC; Mr. Michael Aisenberg (EWA-IIT); Mr. Paul Nicholas (Microsoft); Liesyl Franz (ITAA). Emergency Services: Ms. Ann Davison, Int'l Assoc of Fire Chiefs & Mr. Tom Rhatigan, National Sheriff's Assoc. Homeland Security Program Manager	Sector Coordinating Council Representatives: PCIS Panel: Energy, IT, Commo, Healthcare, Emergency Services

## JUNE 12, 2007

Dr. Til Jolly, Office of Health Affairs, DHS	Pandemics: Community Mitigation and Implications to Planners
Mr. Bill Bryan, Director, DCIP OASD (HD&ASA)	Update on DoD 41 Critical Infrastructure
Mr. Philip Sakowitz, Executive Director, US Army Installation Management Command (Accompanied by Mr. Clay Davis, Mr. Don Stout, Mr. Gordon Rogers)	Installation Preparedness
Oil & Natural Gas: Mr. Gary Forman, NiSource Inc. Highways & Motor Carriers: Martin Rojas, American Trucking Assoc. Railroads: Nancy Wilson, Assoc of American Railroads Transit: Mr. Tom Yedinak, American Public Transportation Association	PCIS Panel: Transportation Sectors

## JUNE 19, 2007

LTG (R) Peter Kind, USA	Y2K Information Coordination Center
Mr. Brandon Wales, DHS	Tier 1 and 2 CI/KR Update
BG Peter Aylward, J34 Antiterrorism and Homeland Defense	WMD Insights
Mr. Jim Schwartz, Arlington County Fire Chief Mr. Marko Bourne, FEMA Dr. Helen Miller, OR-1 Disaster Medical Assistance Team (National Disaster Medical System) Mr. Matt Bettenhausen, California Office of HLS	Panel of State and Local Authorities

**JULY 17, 2007**

Mr. Allan Banghart, DLA Colonel Dennis D'Angelo, TRANSCOM Mr. Alan Estevez, OSD(LM&R)	Logistics Panel: Ensuring Deployment and Supply
LtCol Stephen Hall, USAF, Joint Task Force Civil Support (JTF-CS)	JTF-Civil Support

**Know/Don't Know: Intelligence Panel****FEBRUARY 27, 2007**

Tom Behling, DUSD (I)	How "Persistent Surveillance" Will Work in the Future
-----------------------	---

**MARCH 7, 2007**

Larry Gershwin, NIO for S&T	Unfolding S&T Based Challenges Confronting the military through 2025
Mary Margret Graham, Deputy Director of National Intelligence for Collection	DNI Collection Priorities for the Near Future
Vann H. Van Diepen National Intelligence Office for Weapons of Mass Destruction and Proliferation ODNI/National Intelligence Council	WMD capabilities of all the known and aspiring nuclear (also chem/bio) States

**APRIL 19, 2007**

LTG William Boykin, DUSD Intelligence and Warfighting Support Mr. John W. Perkins, Chief, Special Activities Division at CIA. MG Thomas Csmko, USA Special Forces Command LTG Michael Maples, Dir. DIA	Panel Discussion: "How SOF, HUMINT, and CA Interact to Generate and Use Good Intel"
---	---

**MAY 11, 2007**

Ken Knight, NIO for Warning	National Intelligence Warning System
Mr. Patrick Gorman, ADDNI for Strategy, Plans, and Policy	Results of the QICR (the IC Quadrennial Review)
Don Burke, CIA/DS&T Sean Dennehy, CIA/DI	Intelipedia

**JUNE 12, 2007**

Phil Midland	Insight on China from a Different Perspective
Hank Messick, Bill Miles, & Joe Sepulveda, CIA	Chinese ASAT Launch
Dave Cattler / Josh Kerbel	Navy Deep Red Intel
Dan DeMots/ CDR George Capen	Asia Net Assessment

**Fighting Through Asymmetric Counterforce Panel****FEBRUARY 14, 2007**

GEN Paul Gorman, USA (Ret.)	Military Intelligence Review
-----------------------------	------------------------------

**MARCH 20, 2007**

COL Clay Hicks, USA	Army Asymmetric Warfare
---------------------	-------------------------

**APRIL 26, 2007**

CAPT Sam Neill, USCG	Coast Guard Evergreen Project
LTC Alan Eckersley, USA	Army Irregular Warfare
BG Robin P. Swann, USA	Army Capabilities Integration Center (ARCIC)

**MAY 24, 2007**

Mr. John Plant	Army Asymmetric Warfare
CAPT Mark Mullins, USN	Navy Irregular Warfare / Asymmetric Perspective
Lt Col Tom Dobbs, USAF	Irregular Warfare: Implications for the U.S. Air Force
Mr. Frank Hoffman	Future Warfare: Competing for Influence
Col King, USMC (Ret.)	USMC Perspective: Irregular Warfare Cross-Functional Team

**JUNE 21, 2007**

Maj Gen William Shelton, USAF	AFSPACE, JFCC SPACE, USSTATCOM Brief
Dr. James A. Tegnalia	DTRA Perspective on 21st Century Warfare
Director James Rabon, JIEDDO	Network Centric ISR Fusion Capabilities in Support of Offensive Counterterrorist Operations
RADM Elizabeth Hight, USN	JTF-GNO Brief

CAPT Forbes O. MacVane, USN	Joint Functional Component Command - Network Warfare: Fighting Cyber Adversaries
Dr. Lani Kass	USAF Systems and Connectivity Perspective

**JULY 21, 2007**

Mr. Anthony Bargar	GIG Mission Assurance
Mr. David Aland	Assessment of IA Aspects of COCOM Exercises
Col Steve Luxion, USAF	Q&A USAF Cyber Command
Mr. James Richberg	National Cyber Study Group

**Strategic Communication Panel****MARCH 1, 2007**

Mr. Alberto Fernandez, Director, Middle-East, U.S. Department of State Mr. Thomas Skipper, Director, East Asia and Pacific, U.S. Department of State	Views from the Regional Bureaus
Ms. Gretchen Welch, PPR Director, U.S. Department of State	Policy Plans and Resources (PPR)
Mr. Jeremy Curtin, IIP Coordinator, U.S. Department of State	International Information Programs (IIP)
Mr. Thomas Farrell, Deputy Assistant Secretary for Academic Programs, U.S. Department of State Ms. Chris Miner, Managing Director for Professional and Cultural Exchanges Programs, U.S. Department of State	Educational and Cultural Affairs (ECA)

**MARCH 23, 2007**

Mr. Robert Giesler, USD (Intelligence) Col Glen Ayers, J-39	IO and PSYOPS
RDML Frank Thorp, Director, OASD (Public Affairs) Ms. Alisa Stack-O'Conner, USD (Policy)	Public Affairs and Public Diplomacy
Hon. Ryan Henry, PUSD (Policy) Hon Dorrance Smith, ASD (PA) LTG Walter (Skip) Sharp, DJS JCS	Roundtable Discussion
Mr. Michael Pease, IDA Dr. Caroline Ziemke, IDA	Discussion



## APRIL 13, 2007

Dr. Jon B. Alterman, Director of the Middle East Program at the Center for Strategic and International Studies (CSIS)	The Lexus Hits an Olive Tree
Mr. David Brugger, CEO of Brugger Consulting & Brugger Global Media, former President, Association of America's Public Television Stations (APTS) William Siemering, President, Developing Radio Partners	Community-Based Media
Mr. Kenneth Y. Tomlinson, chairman of U.S. Broadcasting Board of Governors (BBG)	BBG Perspective
Mr. Gary Knell, President and CEO, Sesame Workshop	Sesame Perspective
Mr. Joe Norris, Senior Analyst/Transnational Issues Terrorism/Near East Program, DNI Open Source Center Dr. William C. Hannas, Senior Officer for East Asia S&T, DNI Open Source Center	The Current State of the Arab Media & The China RDA Metadata Mapping Project
Dr. Adam Powell, Director, Integrated Media Systems Center, USC Viterbi School of Engineering	International Broadcasting: Future Trends and Techniques

## MAY 4, 2007

Ms. Mary Lou Jepsen, MIT Media Lab	One Laptop per Child
Mr. Robert Gehorsam, CEO, Forterra Systems Inc.	On Line Gaming
Mr. Ben Gross, Social Technologies Group, UC Berkeley, and UI Urbana-Champaign	Social Technologies
Ms. Susan Gigli, Chief Operating Officer, InterMedia Dr. Haleh Vaziri, Regional Research Manager for Middle East/North Africa, InterMedia	InterMedia
Mr. Mike Pease, IDA	Enemy Use of Immersive Computer Game Technology

## MAY 18, 2005

Mr. Kevin Klose, President, NPR	NPR Perspective
Ms. Jody Olsen, Deputy Director, Peace Corps	Peace Corps Perspective
Mr. James Dobbins, Director, International Security and Defense Policy Center, RAND	Discussion
Professor Jarol B. Manheim, School of Media and Public Affairs, GWU	Social Network Analysis
Mr. Bruce Sherman, BBG Mr. Brian Conniff, BBG	BBG 2008-2013 strategy Radio Sawa & AlHurra TV

## Interviews with Senior Officials

Mr. Peter Bechtel	Strategy, Plans, and Policy Directorate, U.S. Army
Lt. Gen. James L. Campbell	Director of the Army Staff
General James E. Cartwright	Commander, U.S. Strategic Command
General James T. Conway	Commandant, U.S. Marine Corps
Lt Gen David A. Deptula	Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, Headquarters U.S. Air Force
Honorable Eric Edelman	Under Secretary of Defense for Policy
BG Mari K. Eder	Deputy Chief of Public Affairs, U.S. Army
VADM Mark J. Edwards	Deputy Chief of Naval Operations for Communication Networks
Honorable Gordon England	Deputy Secretary of Defense
Admiral Edmund Giambastiani Jr.	Vice Chairman, Joint Chiefs of Staff
Honorable John G. Grimes	Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer
Honorable Francis Harvey	Secretary of the Army
Honorable Ryan Henry	Principal Deputy Under Secretary of Defense for Policy
Dr. Tom Hopkins	Acting Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs
ADM Timothy J. Keating	Commander, U.S. Northern Command
Honorable Ken Krieg	Under Secretary of Defense for Acquisition, Technology, and Logistics
VADM Eric T. Olson	Deputy Commander, U.S. Special Operations Command
Lt.Gen. John F. Sattler	Director for Strategic Plans and Policy, Joint Staff
MG Eric Schoomaker	U.S. Army Medical Research and Materiel Command
General Peter Schoomaker	Chief of Staff, U.S. Army
ADM James Stavridis	Commander, U.S. Southern Command
Dr. James A. Tegnelia	Director, Defense Threat Reduction Agency
Mr. Peter Verga	Assistant Secretary of Defense for Homeland Defense
Honorable Donald Winter	Secretary of the Navy
Honorable Michael Wynne	Secretary of the Air Force
Honorable John Young	Director, Defense Research and Engineering

## Glossary

ASD (HD&ASA)	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
ASD (NII)	Assistant Secretary of Defense for Networks and Information Integration
CGE	Center for Global Engagement
CIO	Chief Information Officer
C4ISR	command, control, communications, and computing and intelligence, surveillance, and reconnaissance
COCOMs	combatant commanders
CONPLAN	concept of operations plan
DARPA	Defense Advanced Research Projects Agency
DCIP	Defense Critical Infrastructure Program
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DOD	Department of Defense
DSB	Defense Science Board
DTRA	Defense Threat Reduction Agency
FFRDC	federally funded research and development center
GEO	geosynchronous earth orbit
GIG	Global Information Grid
GPS	Global Positioning System
HAE UAS	high altitude endurance unmanned aerial system
IED	improvised explosive device
ISR	intelligence, surveillance, and reconnaissance
JPEO	Joint Program Executive Office
LEO	low earth orbit
LTA UAS	lighter than air unmanned aerial system
MEO	mid-earth orbit
NCR	National Capitol Region
NSPD	National Security Presidential Directive
NT-ISR	non-traditional intelligence, surveillance, and reconnaissance
NYPD	New York Police Department
ORS	operationally responsive space
RDD	radiological dispersal device
SERS	surface-enhanced Raman scattering
TRANSCOM	U.S. Transportation Command
UAS	unmanned aerial systems
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology & Logistics
USD (I)	Under Secretary of Defense for Intelligence
USD (P)	Under Secretary of Defense for Policy
WMD	weapons of mass destruction
Y2K	Year 2000



Future of War

Technology

Nuclear Proliferation

Domestic Catastrophe

Deployment and Resupply

Intelligence

Asymmetric Counterforce

Strategic Communication

